ANY.RUN
Interactive malware hunting service

General Info

File name	926e29f9242feb3e11c532616f7c90c5d7acab115d38ebf748cabaaa6a2a3667
Full analysis	
Verdict	Malicious activity
Analysis date	3/2/2020, 09:12:19
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	macros macros-on-open
Indicators:	
MIME:	application/vnd.ms-excel
File info:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Windows User, Last Saved By: RDP, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Sep 27 20:02:20 2018, Last Saved Time/Date: Wed Feb 5 10:50:38 2020, Security: 0
MD5	07D78E211FE6684B999BD9EE46E3BA31
SHA1	894BD5960DBF7D324BB782AE322A0FB65E9E542D
SHA256	926E29F9242FEB3E11C532616F7C90C5D7ACAB115D38EBF748CABAAA6A2A3667
SSDEEP	24576:FLNKXQHOPI1K5SLMKD2RVIEHO/KBHJPYVUVX/+2PPBK:0L4E

Behavior activities

MALICIOUS

Application was dropped or rewritten from another process
- monitor.exe (PID: 3260)
- monitor.exe (PID: 1524)
- monitor.exe (PID: 3020)
- monitor.exe (PID: 2252)
- monitor.exe (PID: 3372)

Starts Visual C# compiler
- monitor.exe (PID: 1524)
- monitor.exe (PID: 3372)
- monitor.exe (PID: 3020)
- monitor.exe (PID: 2252)

Runs app for hidden code execution
- monitor.exe (PID: 3260)
- monitor.exe (PID: 1524)
- monitor.exe (PID: 3372)
- monitor.exe (PID: 3020)
- monitor.exe (PID: 2252)

Changes settings of System certificates
- monitor.exe (PID: 2252)

Loads the Task Scheduler COM API
- EXCEL.EXE (PID: 3076)

Executable content was dropped or overwritten
- EXCEL.EXE (PID: 3076)

SUSPICIOUS

Starts CMD.EXE for commands execution
- monitor.exe (PID: 1524)
- monitor.exe (PID: 3260)
- monitor.exe (PID: 3372)
- monitor.exe (PID: 2252)
- monitor.exe (PID: 3020)

Executed via Task Scheduler
- monitor.exe (PID: 3260)
- monitor.exe (PID: 1524)
- monitor.exe (PID: 3372)
- monitor.exe (PID: 3020)

Executable content was dropped or overwritten
- csc.exe (PID: 2400)

Creates files in the user directory
- notepad++.exe (PID: 1460)

INFO

Manual execution by user
- notepad++.exe (PID: 1460)
- monitor.exe (PID: 2252)
- explorer.exe (PID: 2692)
- explorer.exe (PID: 2128)

Reads Microsoft Office registry keys
- EXCEL.EXE (PID: 3076)

Static information

TRiD

.xls | Microsoft Excel sheet (36.8%)
.xls | Microsoft Excel sheet (alternate) (30%)
.doc | Microsoft Word document (old ver.) (23.3%)

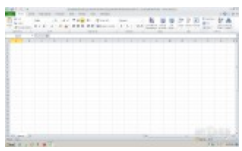
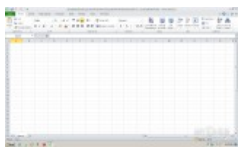
EXIF

FlashPix

Author:	Windows User
LastModifiedBy:	RDP
Software:	Microsoft Excel
CreateDate:	2018:09:27 19:02:20
ModifyDate:	2020:02:05 10:50:38
Security:	None
CodePage:	Windows Latin 1 (Western European)
Company:	*null*
AppVersion:	16
ScaleCrop:	No
LinksUpToDate:	No
SharedDoc:	No
HyperlinksChanged:	No
TitleOfParts:	Sheet2
HeadingPairs	*null*
	null
CompObjUserTypeLen:	31
CompObjUserType:	Microsoft Excel 2003 Worksheet

Screenshots

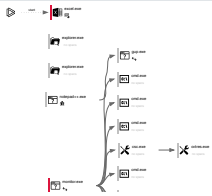


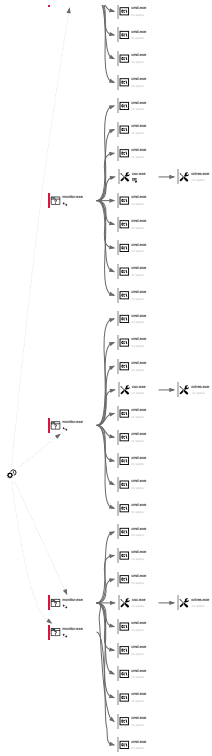





Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
130	51	6	0

Behavior graph





Registry activity

Total events	Read events	Write events	Delete events
1413	1196	209	8

Modification events

PID	Process	Operation	Key	Name	Value
3076	EXCEL.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems		
3076	EXCEL.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency		
3076	EXCEL.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A686DD		
3076	EXCEL.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery		
3076	EXCEL.EXE	delete key	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A68854		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	)v0	29763000040C0000010000000000000000000000
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1041	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1046	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1036	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1031	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1040	Off

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1049	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	3082	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1042	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1055	Off
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1033	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1046	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1036	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1031	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1040	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1041	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1049	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	3082	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1042	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages	1055	On
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{0C12CF48-451D-45AC-A927-F5FDBFC07C96}		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{9C3CFE2A-537A-479A-A1E2-85728C400F7D}		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{A8716C2B-35ED-4EE7-A138-FBA0A7C9B5B0}		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{AA3BD3AB-AD94-4243-86C5-8AE3D7D829BC}		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{BC29864C-2254-4A9E-9F4D-721A388618BB}		
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\User Settings\Kosmarttag_SmartTag	Count	1
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel	MTTT	040C000068F6DA576AF0D50100000000
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	0
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	1
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A686DD	A686DD	

04000000040C00006600000043003A005C005500730065007200730005C00610064006D0069006E005C00410070007000440061007400610005C004C006F006300610
06C005C00540065006D0070005C00390032003600650032003900660039003200340032006600650062003300650031003100630035003300320036003100360066
0037006300390030006300350064003700610063006100620031003100350064003300380065006200660037003400380063006100620061006100610036006100320
0610033003600360037002E0078006C00730000000000220000043003A005C005500730065007200730005C00610064006D0069006E005C00410070007000440061
0740061005C004C006F00630061006C005C00540065006D0070005C000100000000000000801CCE586AF0D501DD86A600DD86A600000000000AC0200000010000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A686DD	A686DD	

04000000040C00006600000043003A005C0055007300650072007300 5C00610064006D0069006E005C00410070007000440061007400610 05C004C006F006300610
06C005C00540065006D0070005C00390032003600650032003900660039003200340032006600650062003300650031003100630035003300320036003100360066 0
03700630039003000630035006400370061006300610062003100310035006400330038006500620066003700340038006300610062006100610061003600610032 00
610033003600360037002E0078006C0073000000000002200000004 3003A005C0055007300650072007300 5C00610064006D0069006E005C0041007000700044 00610
0740061005C004C006F00630061006C005C00540065006D0070005C000100000000000000801CCE586AF0D501DD86A600DD86A60000000000AC0200000018000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000

3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	EXCELFiles	1348599839
3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1348599989
3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	VBAFiles	1348599815
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A686DD	A686DD	

04000000040C00006600000043003A005C0055007300650072007300 5C00610064006D0069006E005C00410070007000440061007400610 05C004C006F006300610
06C005C00540065006D0070005C00390032003600650032003900660039003200340032006600650062003300650031003100630035003300320036003100360066 0
03700630039003000630035006400370061006300610062003100310035006400330038006500620066003700340038006300610062006100610061003600610032 00
610033003600360037002E0078006C0073000000000002200000004 3003A005C0055007300650072007300 5C00610064006D0069006E005C0041007000700044 00610
0740061005C004C006F00630061006C005C00540065006D0070005C000100000000000000801CCE586AF0D501DD86A600DD86A60000000000AC0200000018000
0040000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\A68854	A68854	

04000000040C00006600000043003A005C0055007300650072007300 5C00610064006D0069006E005C00410070007000440061007400610 05C004C006F006300610
06C005C00540065006D0070005C00390032003600650032003900660039003200340032006600650062003300650031003100630035003300320036003100360066 0
03700630039003000630035006400370061006300610062003100310035006400330038006500620066003700340038006300610062006100610061003600610032 00
610033003600360037002E0078006C0073000000000002200000004 3003A005C0055007300650072007300 5C00610064006D0069006E005C0041007000700044 00610
0740061005C004C006F00630061006C005C00540065006D0070005C0001000000010000004CA8CC576AF0D5015488A6005488A60000000000AC0200006E00000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	25

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Item 1	
[F00000000][T01D56F99396E0A50][O00000000]*C:\Users\admin\Documents\					
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU	Max Display	25
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU	Item 1	
[F00000000][T01D56F99396E0A50][O00000000]*C:\Users\admin\Documents\test.xlsx					
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{DCB24385-F59F-4B3D-83CD-56ACAEB32E6F}\2.0		Microsoft Forms 2.0 Object Library
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{DCB24385-F59F-4B3D-83CD-56ACAEB32E6F}\2.0\FLAGS		6
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{DCB24385-F59F-4B3D-83CD-56ACAEB32E6F}\2.0\0\win32		
C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd					
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\TypeLib\{DCB24385-F59F-4B3D-83CD-56ACAEB32E6F}\2.0\HELPDIR		C:\Users\admin\AppData\Local\Temp\VBE
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{BEF6E003-A874-101A-8BBA-00AA00300CAB}		Font
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{EC72F590-F375-11CE-B9E8-00AA006B1A69}		IDataAutoWrapper
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02370-B5BC-11CF-810F-00A0C9030074}		IReturnInteger
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02371-B5BC-11CF-810F-00A0C9030074}		IReturnBoolean
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{82B02372-B5BC-11CF-810F-00A0C9030074}		IReturnString
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8A683C90-BA84-11CF-8110-00A0C9030074}		IReturnSingle
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8A683C91-BA84-11CF-8110-00A0C9030074}		IReturnEffect
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC6-866C-11CF-AB7C-00AA00C08FCF}		IControl
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC7-866C-11CF-AB7C-00AA00C08FCF}		Controls
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{29B86A70-F52E-11CE-9BCE-00AA00608E01}		IOptionFrame
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC8-866C-11CF-AB7C-00AA00C08FCF}		_UserForm
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{9A4BBF53-4E46-101B-8BBD-00AA003E3B29}		ControlEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5B9D8FC8-4A71-101B-97A6-00000B65C08B}		FormEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{CF3F94A0-F546-11CE-9BCE-00AA00608E01}		OptionFrameEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC1-866C-11CF-AB7C-00AA00C08FCF}		ILabelControl
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC4-866C-11CF-AB7C-00AA00C08FCF}		ICommandButton
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D13-EC42-11CE-9E0D-00AA006002F3}		IMdcText
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D23-EC42-11CE-9E0D-00AA006002F3}		IMdcList
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D33-EC42-11CE-9E0D-00AA006002F3}		IMdcCombo
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D43-EC42-11CE-9E0D-00AA006002F3}		IMdcCheckBox
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D53-EC42-11CE-9E0D-00AA006002F3}		IMdcOptionButton

3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D63-EC42-11CE-9E0D-00AA006002F3}	IMdcToggleButton
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC3-866C-11CF-AB7C-00AA00C08FCF}	IScrollbar
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{A38BFFC3-A5A0-11CE-8107-00AA00611080}	Tab
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{944ACF93-A1E6-11CE-8104-00AA00611080}	Tabs
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC2-866C-11CF-AB7C-00AA00C08FCF}	ITabStrip
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{79176FB3-B7F2-11CE-97EF-00AA006D2776}	ISpinbutton
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{4C599243-6926-101B-9992-00000B65C6F9}	IImage
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D111-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLSubmitButton
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D113-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLImage
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D115-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLReset
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D117-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLCheckbox
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D119-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLOption
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11B-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLText
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11D-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLHidden
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D11F-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLPassword
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D123-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLSelect
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5512D125-5CC6-11CF-8D67-00AA00BDCE1D}	IWHTMLTextArea
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{978C9E22-D4B0-11CE-BF2D-00AA003F40D0}	LabelControlEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC1-AF6C-11CE-9F46-00AA00574A4F}	CommandButtonEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D12-EC42-11CE-9E0D-00AA006002F3}	MdcTextEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D22-EC42-11CE-9E0D-00AA006002F3}	MdcListEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D32-EC42-11CE-9E0D-00AA006002F3}	MdcComboEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D42-EC42-11CE-9E0D-00AA006002F3}	MdcCheckBoxEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D52-EC42-11CE-9E0D-00AA006002F3}	MdcOptionButtonEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{8BD21D62-EC42-11CE-9E0D-00AA006002F3}	MdcToggleButtonEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC2-AF6C-11CE-9F46-00AA00574A4F}	ScrollbarEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC7-AF6C-11CE-9F46-00AA00574A4F}	TabStripEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{79176FB2-B7F2-11CE-97EF-00AA006D2776}	SpinbuttonEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{4C5992A5-6926-101B-9992-00000B65C6F9}	ImageEvents
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{796ED650-5FE9-11CF-8D68-00AA00BDCE1D}	WHTMLControlEvents

3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE0-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents1
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE1-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents2
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE2-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents3
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE3-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents4
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE4-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents5
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE5-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents6
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE6-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents7
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE8-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents9
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{47FF8FE9-6198-11CF-8CE8-00AA006CB389}		WHTMLControlEvents10
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{5CEF5613-713D-11CE-80C9-00AA00611080}		IPage
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{92E11A03-7358-11CE-80CB-00AA00611080}		Pages
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{04598FC9-866C-11CF-AB7C-00AA00C08FCF}		IMultiPage
3076	EXCEL.EXE	write	HKEY_CLASSES_ROOT\Interface\{7B020EC8-AF6C-11CE-9F46-00AA00574A4F}		MultiPageEvents
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Licensing	538F6C892AD540068154C6670774E980	

0100000027000000 7B39303134303030302D303033442D303030302D303030302D303030303030304646314345 7D005A0000004F006600660069006300650020003 10034002C0020004F006600660069006300650050007200 6F006600650073007300690006F006E0061006C002D005200650074006100690006C002000650064006900 740069006F006E000000

3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	XDOCSEditorFiles	1348599809
3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	1348599824
3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109E60090400000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	1348599825
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	PropertiesWindow	4 23 180 640 1
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	StickyPtX	639
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options	StickyPtY	349
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MainWindow	0 0 1280 692 1
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	MdiMaximized	0
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Dock	

02004C01050008000400 1700FC04B002FF02010104001700B800B002FF02000104001700B8000E01050000010400 1401B800B00201000001BE001700FC04B002F F020001BE001700FC04B002FF020101BE001700FC04B00200000001BB035E00FC03FC0206000000D300AF0109033202FF030100D300AF0109033202040000009 301AF0109033202030000000D300AF0109033202020000000210072016C021202FF03010021007201E800120204000000EE007201A901120203000000AF0172016C02 120202000000F8028100AC030101050000005900300 20D014B03010000003A03BC0079031F02060000001600 1600D901C400040001002C002C00EB01E30003000 100420042003B02F700020001000000000000000000000800000058005700 3701FF0101000100000000000000000000600 01006E006E007F01520105000100000000000 000000000000100

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	FolderView	1
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	Tool	

00000000070000047656E6572616C00FFFFFFFFFFFFFFFF

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	CtlsShowSelected	0
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	DsnShowSelected	0
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Toolbars\Settings	Microsoft Visual Basic	

0101000000000000120001000000201FFFF8F0500000100180000001000000020002FE00000000C800000005401AD001C02A1020201FFFF22070000080100000001
10000030103FE00000000000000009A01F3009A01F3000201FFFF2908000005011800000010000001000 1FE00000000000078 00BD011601B1038E010201FFFF2F0
8000041011800000010000000000FE00000000C8000000E001C000A802B4020201FFFF9A06000041011800000010000002000 2FE00000000C80000000302C000C
B02B4020201FFFFBD06000041011800000010000002000 2FE00000000C80000002602C000EE02B4020201FFFF650700004101180000001000000 20002FE0000000
0C80000004902C0001103B4020201FFFF270800004101180000001000000 20002FE00000000C80000006C02C0003403B4020201FFFFFC0600000101180000000100
000020002FE00000000C80000006801AD003002A1020201FFFFF10500004101180000001000000 2002FE00000000090100008B01C0009402B4020201FFFF9A080
0004101180000001000000 2002FE00000000C8000000D101C0009902B4020201FFFF46070000410118000000100000020002FE00000000000000F4013901F401
39010201FFFFF00600004101180000001000000 2002FE00000000000000017025C0117025C010201FFFFA708000041011800000010000002000 2FE00000000C80
000003A02C0000203B4020201FFFF1C07000010118000000100000020002FE00000000C80000005D02C0002503B4020201FFFFF10600004101180000001000000
20002FE00000000C80000008002C0004803B4020201FFFFD506000041011800000010000002000 2FE00000000C80000007C01AD004402A1020201FFFF880900004
101180000001000000 2002FE00000000C80000009F01C0006702B402

3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	UI	

6800000001010000000000000600010000000 2010B000080000008010001000014000 84D0065006E007500200042006100720001010100000 0FFFF0000FDFF32003
20058025A000000000000301200A3275000008000301000000000180000000301200A33750000080003020000000002800000030 1200A34750000080003030000000 0
3800000030 1200A3575000008000304000000000480000000301200A3675000008000305000000000580000000301200AD57500000800030600000000068000000301 2
00A3C7500000800030700000000078000000301200A3775000008000308000000000880000000301200A56750000080003090000000098000000301200A397500000
800030A000000000A8000000301200A3A7500000800030B000000030000000000201FFFF2F8000000000000000010000853007400610 06E0064006100720064000 1
0101010000FFFF0000FDFF32006E00580296002F0000000201FFFF308000000000000000000100004450064006900740004000 1020000FFFF0000FDFF3200AA0058
02D2003000000000201FFFF3180000000000000000010000544006500620075006700040001030000FFFF0000FDFF3200E60058020E013100000000201FFFF3280000
0000000000000100008550073006500720046006F0072006D00040001040000FFFF0000FDFF3200220158024A01320000000201FFFFDB0000009701000200001000
0004000101000000000000000000000000000000042000000

3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1348599990
3076	EXCEL.EXE	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000000000000F01FEC\Usage	ProductFiles	1348599991
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel	MTTF	90
3076	EXCEL.EXE	write	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel	MTTA	90
1460	notepad++.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US
1460	notepad++.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	UNCAsIntranet	0
1460	notepad++.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap	AutoDetect	1
3020	monitor.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	EnableFileTracing	0
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	EnableConsoleTracing	0
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	FileTracingMask	4294901760
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	ConsoleTracingMask	4294901760
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	MaxFileSize	1048576
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASAPI32	FileDirectory	%windir%\tracing
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	EnableFileTracing	0
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	EnableConsoleTracing	0

2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	FileTracingMask	4294901760
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	ConsoleTracingMask	4294901760
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	MaxFileSize	1048576
2252	monitor.exe	write	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\monitor_RASMANCS	FileDirectory	%windir%\tracing
2252	monitor.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US
2252	monitor.exe	write	HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\CA\Certificates\1FB86B1168EC743154062E8C9CC5B171A4B7CCB4	Blob	

030000000100000001400000001FB86B1168EC743154062E8C9CC5B171A4B7CCB4140000000010000001400000000F80611C823161D52F28E78D4638B42CE1C6D9E
204000000010000001000000000345EFF15B7A49ADD451B65A7F4BDC6AE0F000000010000002000000010D93C9864A521F3065CC3A522509C2AFABB01581CAD9
C6D8E89FDD75F9EA74719000000010000001000000E476DC02F1CECF7E6C1E756CD803F6261800000001000000100000000F3A0527D242DE2DC98E5CFCB1
E991EE200000000100000098040000308204943082037CA003020102021001FDA3EB6ECA75C888438B724BCFBC91300D06092A864886F70D01010B0500306131
0B3009060355040613025553311530136035504 0A130C44696769436572742049 6E6331193017060355040B13107777772E64696769636572742E636F6D3120301
E060355040313174469676943657272 0420476C6F62616C20526F6F74204341301E170D3133303330383132303030305A170D3233303330383132303030305A304D31
0B3009060355040613025553311530136035504 0A130C44696769436572742049 6E6331273025060355040313 1E44696769436572742053484132205365637265
20536572766572204341308201223000D06092A864886F70D01010500038201 0F003082010A0282010100DCAE58904DC1C4301590355B6E3C8215F52C5CBDE3
DBFF7143FA642580D4EE18A24DF066D00A736E1198361764AF379DFDFA4184AFC7AF8CFE1A734DCF339790A2968753832BB9A675482D1D56377BDA31321A
D7ACAB06F4AA5D4BB74746DD2A93C3902E798080EF13046A143BB59B92BEC207654EFCDAFCFF7AAEDC5C7E55310CE83907A4D7BE2FD30B6AD2B1DF5FF
E5774533B3580DDAE8E4498B39F0ED3DAE0D7F46B29AB44A74B58846D924B81C3DA738B129748900445751ADD37319792E8CD540D3BE4C13F395E2EB8F35
C7E108E8641008D456647B0A165CEA0AA29094EF397EBE82EAB0F72A7300EFAC7F4FD1477C3A45B2857C2B3F982FDB745589B0203010001A382015A308201
5630120603551D130101FF040830060101FF020100300E0603551D0F0101FF040403020186303406082B0601050507010104283026302406082B060105050730018
618687474703A2F2F6F6373702E64696769636572742E636F6D307B0603551D1F047430723037A035A033863168747 4703A2F2F63726C332E64696769636572742
E636F6D2F44696769436572 74476C6F62616C526F6F7443412E63726C3037A035A033863168747 4703A2F2F63726C342E64696769636572742E636F6D2F446967
6943657274476C6F62616C526F6F7443412E63726C303D0603551D20043603034303 20604551D2000302A302806082B0601050507020116 1C68747470733A2F2F77
7772E64696769636572742E636F6D2F435053301D0603551D0E041604140F80611C823161D52F28E78D4638B42CE1C6D9E2301F0603551D2304183016801403
DE503556D14CBB66F0A3E21B1BC397B23DD155300D06092A864886F70D01010B05000382010100233EDF4BD23142A5B67E425C1A44CC69D168B45D4BE0042
16C4BE26DCCB1E0978FA65309CDAA2A65E5394F1E83A56E5C98A22426E6FBA1ED93C72E02C64D4ABFB042DF78DAB3A8F96DFF21855336604C76CEEC38D
CD65180F0C5D6E5D44D2764AB9BC73E71FB4897B8336DC91307EE96A21B1815F65C4C40EDB3C2ECFF71C1E347FFD4B900B43742DA20C9EA6E8AEE1406A
E7DA2599888A81B6F2DF4F2C9145F26CF2C8D7EED37C0A9D539B982BF190CEA34AF002168F8AD73E2C932DA38250B55D39A1DF06886ED2E4134EF7CA550
1DBF3AF9D3C1080CE6ED1E8A5825E4B877AD2D6EF552DDB4748FAB492E9D3B9334281F78CE94EAC7BDD3C96D1CDE5C32F3

3372	monitor.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US
1524	monitor.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US
3260	monitor.exe	write	HKEY_CLASSES_ROOT\Local Settings\MuiCache\12B\52C64B7E	LanguageList	en-US

Files activity

Executable files	Suspicious files	Text files	Unknown types
3	2	45	2

Dropped files

PID	Process	Filename	Type
2400	csc.exe	C:\Users\admin\AppData\Local\Temp\lsyj0klv.dll	executable
		MD5: 8BB85F5A477C0A11A7729AE1C9164B79 **SHA256:** 621674C086DDCBE959B266AA16536CE9A1325A5CB543583A2A05	
3076	EXCEL.EXE	C:\Users\public\.Monitor\monitor.xls	executable
		MD5: B08DFF2A95426A0E32731EF337EAB542 **SHA256:** EBAE23BE2E24139245CC32CEDA4B05C77BA393442482109CC69A	
3076	EXCEL.EXE	C:\Users\public\.Monitor\monitor.exe	executable
		MD5: B08DFF2A95426A0E32731EF337EAB542 **SHA256:** EBAE23BE2E24139245CC32CEDA4B05C77BA393442482109CC69A	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt	text
		MD5: 87A2C1B15C25BF90D0A16D257BA7E485 **SHA256:** B58FA7A55798BF658E8434717DB844A5DD668AA3638AA5177151B	
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text

		MD5: 49684103E5D67ED4FD32A9ECDEB169C7	**SHA256:** 76F26D02306156C76C3F965CED00B3DE93E47065E48A4010547C8
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 327130CB986DD09C24B6A9CEB5B0CC92	**SHA256:** 66EEBAEAFCCA0CDD0FFA1A2ECC7B258A53A32724371C73A2237
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: BB6D218975DA6580623167E4CBA9888D	**SHA256:** 19AF70FFC21F5D7240850833357EA5B81DCB9CBEF906F720A11D52
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: E455AE583D69AA309965737FE65E1BA1	**SHA256:** A134E6C83FAF46DCD10DA9668B7D4823F4F957D87A6AAD62378C
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 4C3AC1199BE46FC3AEB3DD6E5596DF…	**SHA256:** 390E7362B63955F57871D1D11FD3740BE0A15D7C956FC643ECE29
2600	csc.exe	C:\Users\admin\AppData\Local\Temp\qpbtmmzo.out	—
		MD5: —	**SHA256:** —
2600	csc.exe	C:\Users\admin\AppData\Local\Temp\qpbtmmzo.dll	—
		MD5: —	**SHA256:** —
1140	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RESBB37.tmp	—
		MD5: —	**SHA256:** —
2600	csc.exe	C:\Users\admin\AppData\Local\Temp\CSCBB36.tmp	—
		MD5: —	**SHA256:** —
1524	monitor.exe	C:\Users\admin\AppData\Local\Temp\qpbtmmzo.cmdline	—
		MD5: —	**SHA256:** —
1524	monitor.exe	C:\Users\admin\AppData\Local\Temp\qpbtmmzo.0.cs	—
		MD5: —	**SHA256:** —
3372	monitor.exe	C:\Users\public\.Monitor\ews.conf	text
		MD5: CABD5D1691394EF020E965CC608BF0C2	**SHA256:** 1B2C5354EB567132A341C1B15AD5CC71C3F5BA8E2788B67C0FB0
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: E34FA9D73D52BF8E6B927983B7BDA04E	**SHA256:** B7E564667A5F64A56BFE5A96DF84371BCD591FA00A0D6D36B5E1
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: D81D1E95D92333240AB09166E0382361	**SHA256:** 76ABA50CDDBF23E25F1C47945C4CE105989356DB19C2A00330B4
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 9AAA48E62AEED81528EFE65A8ED56100	**SHA256:** 34784BCEEDDE3FDE43049858EF900D70643460A22A131F96898E1
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 7E5C792FB92A4ADD8DCCEC4CE6285…	**SHA256:** 39ED200446727D6238C5A85E3A58C7EA9628124E25F2A366E37B3
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: AE8904ED44D3076AFCADD8BE36B7F8E6	**SHA256:** 3F080CD9451ED56670F590F7F2A36A5C1BB2EB9535CA94801B394
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: A1FEB5452161978C427F497B1E880706	**SHA256:** 31926BD43A508D542DCA03213F66FC8F6EC00B9368589845888CF
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: FC892ABD73F15FAF65E09DBC6695A9E8	**SHA256:** F789B6B74B21737933324E3ED47087E3746AA1B95DF57DBBBD7E
3372	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 2498C6C9B8A0D7C73970FA471F211513	**SHA256:** AD3F1276788ECA62C6A92EF92C7B94584026480268EB8D7D5F86E
2528	csc.exe	C:\Users\admin\AppData\Local\Temp\gdzl7abt.out	—
		MD5: —	**SHA256:** —
2528	csc.exe	C:\Users\admin\AppData\Local\Temp\gdzl7abt.dll	—
		MD5: —	**SHA256:** —
3776	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RES4253.tmp	—
		MD5: —	**SHA256:** —
2528	csc.exe	C:\Users\admin\AppData\Local\Temp\CSC4252.tmp	—
		MD5: —	**SHA256:** —
3372	monitor.exe	C:\Users\admin\AppData\Local\Temp\gdzl7abt.cmdline	—

		MD5: —	**SHA256:** —	
3372	monitor.exe	C:\Users\admin\AppData\Local\Temp\gdzl7abt.0.cs		—
		MD5: —	**SHA256:** —	
3020	monitor.exe	C:\Users\public\.Monitor\ews.conf		text
		MD5: CABD5D1691394EF020E965CC608BF0C2	**SHA256:** 1B2C5354EB567132A341C1B15AD5CC71C3F5BA8E2788B67C0FB0	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 76B43F337122F33784E259B5314C33A0	**SHA256:** B20EBCE23CA655682D8047F3AAC4E1BE685AB14DDFB27B4C686	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: A2745BEE98B133D30C728DA6CD020144	**SHA256:** 7CDD8D24B1BEB215852F575D265A5B44D15F381C522509F5510E9	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 872991AFB89066A556C90577668C9FAA	**SHA256:** 33C9A22E177068A59285C5DA13023DDD5DB4C9E9A3072DFEDC7	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 969A13997CF8C1F6349258B39D8AD91D	**SHA256:** 43416A82AE489653DC037AEDD727A25E7EA81723ABB774996E9B	
2252	monitor.exe	C:\Users\Public\.Monitor\ews.conf		text
		MD5: CABD5D1691394EF020E965CC608BF0C2	**SHA256:** 1B2C5354EB567132A341C1B15AD5CC71C3F5BA8E2788B67C0FB0	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text
		MD5: 531178EA1884FF0EA15DC60EAAA43D7E	**SHA256:** A4B3A3EDBFBAD20E52C66CB3D84A5E93400254493255CFEAADA	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 273EF80B19AB9F96B550C6065BA6D9D7	**SHA256:** 0BA47A2EF331BF1F903C50FCD14483D94566FA3DC8202F2FAD2C	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\CVR8209.tmp.cvr		—
		MD5: —	**SHA256:** —	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 87A2C1B15C25BF90D0A16D257BA7E485	**SHA256:** B58FA7A55798BF658E8434717DB844A5DD668AA3638AA5177151B	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text
		MD5: D1B93E90FEB5D7BA03D1BACDAD0EF…	**SHA256:** 5203D8ADBDCC0F8E880515CD60808B74D57F29FB93130D9EC6B4	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: D1B93E90FEB5D7BA03D1BACDAD0EF…	**SHA256:** 5203D8ADBDCC0F8E880515CD60808B74D57F29FB93130D9EC6B4	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text
		MD5: 98984EC03A91F347B0002E402EC1EBF7	**SHA256:** 5DD9A6029FD72E6AEB47B88D855DE1D2F571218BED12B66B68FE	
3020	monitor.exe	C:\Users\public\.Monitor\e.txt		text
		MD5: 98984EC03A91F347B0002E402EC1EBF7	**SHA256:** 5DD9A6029FD72E6AEB47B88D855DE1D2F571218BED12B66B68FE	
3248	csc.exe	C:\Users\admin\AppData\Local\Temp\w0o-xkjq.out		—
		MD5: —	**SHA256:** —	
3248	csc.exe	C:\Users\admin\AppData\Local\Temp\w0o-xkjq.dll		—
		MD5: —	**SHA256:** —	
3104	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RESD263.tmp		—
		MD5: —	**SHA256:** —	
3248	csc.exe	C:\Users\admin\AppData\Local\Temp\CSCD262.tmp		—
		MD5: —	**SHA256:** —	
3020	monitor.exe	C:\Users\admin\AppData\Local\Temp\w0o-xkjq.0.cs		—
		MD5: —	**SHA256:** —	
3020	monitor.exe	C:\Users\admin\AppData\Local\Temp\w0o-xkjq.cmdline		—
		MD5: —	**SHA256:** —	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text
		MD5: 5BBECAB61632AC3E58A7EC0C03650D27	**SHA256:** 2C16F7A83100522D26CFD170F338453E2800841691A10A79793662	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text
		MD5: 6CFADDB5313861C92057ED386E5EBC5D	**SHA256:** AC8D0D7C6ABE78573758E78539045C4EBDE7C1E5AFAA32C9EF6	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt		text

		MD5: F0B819F42121A995434803DC2C02A7E4 **SHA256:** 36DF78E3B2A6589E9777F9610689D0A1961C6663757B3B3C13B28	
2252	monitor.exe	C:\Users\Public\.Monitor\e.txt	text
		MD5: 598E4F5F0D54A38B21FA62695F677E85 **SHA256:** 6EABFBE8D21B108C0DEE51F53BF8795E9C681844BC07B9F8A726	
2400	csc.exe	C:\Users\admin\AppData\Local\Temp\lsyj0klv.out	—
		MD5: — **SHA256:** —	
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 118CED308EB60CD03D9BA40742FD44C3 **SHA256:** E8044B19CCB35B888E174E95AD303A05097875DB997EA9BA007E	
1756	cvtres.exe	C:\Users\admin\AppData\Local\Temp\RESBFF4.tmp	—
		MD5: — **SHA256:** —	
2400	csc.exe	C:\Users\admin\AppData\Local\Temp\CSCBFF3.tmp	—
		MD5: — **SHA256:** —	
2252	monitor.exe	C:\Users\admin\AppData\Local\Temp\lsyj0klv.cmdline	text
		MD5: 91A73731E535195F169DA0F6A197B0EA **SHA256:** 8FF490B71564843BA20C4B707F16B717FA78A56BB03263856E5369	
2252	monitor.exe	C:\Users\admin\AppData\Local\Temp\lsyj0klv.0.cs	text
		MD5: CC58CCFA5A7514C0B11102BFE173EC58 **SHA256:** 0B4D38C82E229C54A7A3F937FE0020BCCD07FF1EAB83109957A2	
2252	monitor.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B7C322D57057B3593664F2D411D5C076	binary
		MD5: 0416DDFC20DD656E300D19B5A86C47D5 **SHA256:** DEB4D91EF1B350FFC3FD2DCA34247A0EC1DC858B6B4FA959FEA	
2252	monitor.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B7C322D57057B3593664F2D411D5C076	der
		MD5: 345EFF15B7A49ADD451B65A7F4BDC6AE **SHA256:** 154C433C491929C5EF686E838E323664A00E6A0D822CCC958FB4D	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\session.xml	text
		MD5: 0939574012A454C1CCB64A5E091F3E4E **SHA256:** 27A6E967EBB786FE6A1039B55A7E8B414E86E704F22802D7ADD5	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\config.xml	xml
		MD5: 97CDA314267B260E7B2240013B807975 **SHA256:** 87EE1EBBC4E21213C7F5B08A8065F80197A628801AA7440A27D7E	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\plugins\Config\converter.ini	text
		MD5: F70F579156C93B097E656CABA577A5C9 **SHA256:** B926498A19CA95DC28964B7336E5847107DD3C0F52C85195C135D	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\shortcuts.xml	text
		MD5: AD21A64014891793DD9B21D835278F36 **SHA256:** C24699C9D00ABDD510140FE1B2ACE97BFC70D8B21BF3462DED8	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\stylers.xml	xml
		MD5: 44982E1D48434C0AB3E8277E322DD1E4 **SHA256:** 3E661D3F1FF3977B022A0ACC26B840B5E57D600BC03DCFC6BEF	
1460	notepad++.exe	C:\Users\admin\AppData\Roaming\Notepad++\langs.xml	xml
		MD5: E792264BEC29005B9044A435FBA185AB **SHA256:** 5298FD2F119C43D04F6CF831F379EC25B4156192278E40E458EC3	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\~DFB46C70466B32A9B3.TMP	—
		MD5: — **SHA256:** —	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\~DFA38F0225CCE72B56.TMP	—
		MD5: — **SHA256:** —	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\926e29f9242feb3e11c532616f7c90c5d7acab115d38ebf748cabaaa6a2a3667.xls	document
		MD5: 865903974ED7C1956C2BFDBF6D2D5852 **SHA256:** 9840673B49F4E1EC1E83211CA487FF0E10A7B65066F356EA94766	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\~DF2446E2AA56DBDDE6.TMP	—
		MD5: — **SHA256:** —	
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: 1234E9BA97F9F6E7CF8741F99589B4B0 **SHA256:** 08294E532E80CD380A9F5805D08E9E58DEF3E23D1BBE54EABE09	
1524	monitor.exe	C:\Users\public\.Monitor\e.txt	text
		MD5: B58FCC8D5AC405861CAAFBC33641E540 **SHA256:** 3B82D8A7C52EB056CC1E9A1ADC4147418D5961EDF0F27C29190E	
3076	EXCEL.EXE	C:\Users\public\.Monitor\monitor.exe.config	xml
		MD5: 48D22038C7E7CC968A2CB6FB39519E11 **SHA256:** 678D59BCD469E4CF236C7AF7517C54AB9AD643523383875BD875	
3076	EXCEL.EXE	C:\Users\admin\AppData\Local\Temp\VBE\MSForms.exd	tlb
		MD5: F97B41D434AF302D3ECB9D2C39668DE6 **SHA256:** 32002243891479A23DEEAEDD0D1546275A27F38CA14213E0A75BA	

1524	monitor.exe	C:\Users\public\.Monitor\ews.conf	text

MD5: CABD5D1691394EF020E965CC608BF0C2 **SHA256:** 1B2C5354EB567132A341C1B15AD5CC71C3F5BA8E2788B67C0FB0

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
2	69	5	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
—	—	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA%2Fz5hY5qj0aEmX0H4s05bY%3D	US	der	1.47 Kb	whitelisted
2252	monitor.exe	GET	200	104.18.11.39:80	http://cacerts.digicert.com/DigiCertSHA2SecureServerCA.crt	US	der	1.15 Kb	whitelisted

Connections

PID	Process	IP	ASN	CN	Reputation
1876	gup.exe	104.31.89.28:443	Cloudflare Inc	US	shared
—	—	93.184.220.29:80	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
2252	monitor.exe	185.12.220.8:443	Waves S.a.l	LB	unknown
2252	monitor.exe	104.18.11.39:80	Cloudflare Inc	US	shared
3020	monitor.exe	185.12.220.8:443	Waves S.a.l	LB	unknown
3372	monitor.exe	185.12.220.8:443	Waves S.a.l	LB	unknown
1524	monitor.exe	185.12.220.8:443	Waves S.a.l	LB	unknown
3260	monitor.exe	185.12.220.8:443	Waves S.a.l	LB	unknown

DNS requests

Domain	IP	Reputation
notepad-plus-plus.org	104.31.89.28 104.31.88.28	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
mail.general-security.gov.lb	185.12.220.8	unknown
cacerts.digicert.com	104.18.11.39 104.18.10.39	whitelisted
_kerberos._tcp.dc._msdcs.dgsg.local	No response	unknown

Threats

No threats detected.

Debug output strings

Process	Message
notepad++.exe	42C4C5846BB675C74E2B2C90C69AB44366401093
notepad++.exe	42C4C5846BB675C74E2B2C90C69AB44366401093
notepad++.exe	42C4C5846BB675C74E2B2C90C69AB44366401093