ID: 427681
Sample Name:
document230134.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:17:57
Date: 01/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

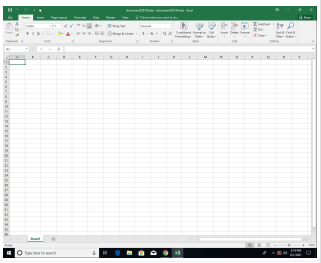
Analysis Report document230134.xlsx

Overview

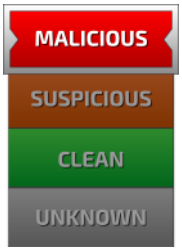
General Information

Sample Name:	document230134.xlsx
Analysis ID:	427681
MD5:	badd03190784a6..
SHA1:	5bb5f2ca6419e2e.
SHA256:	16b1d0cbb8eb48..
Infos:	

Most interesting Screenshot:



Detection



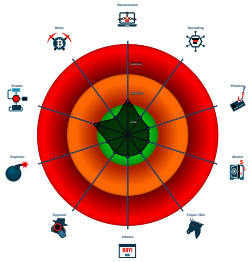
Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm…

Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 3636 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

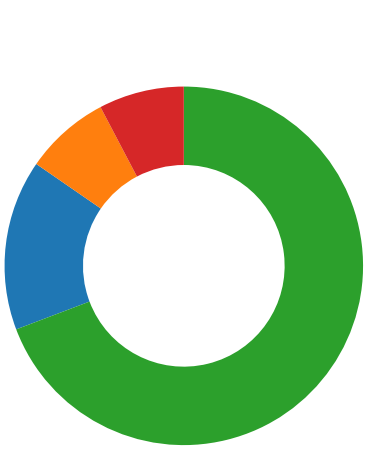
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

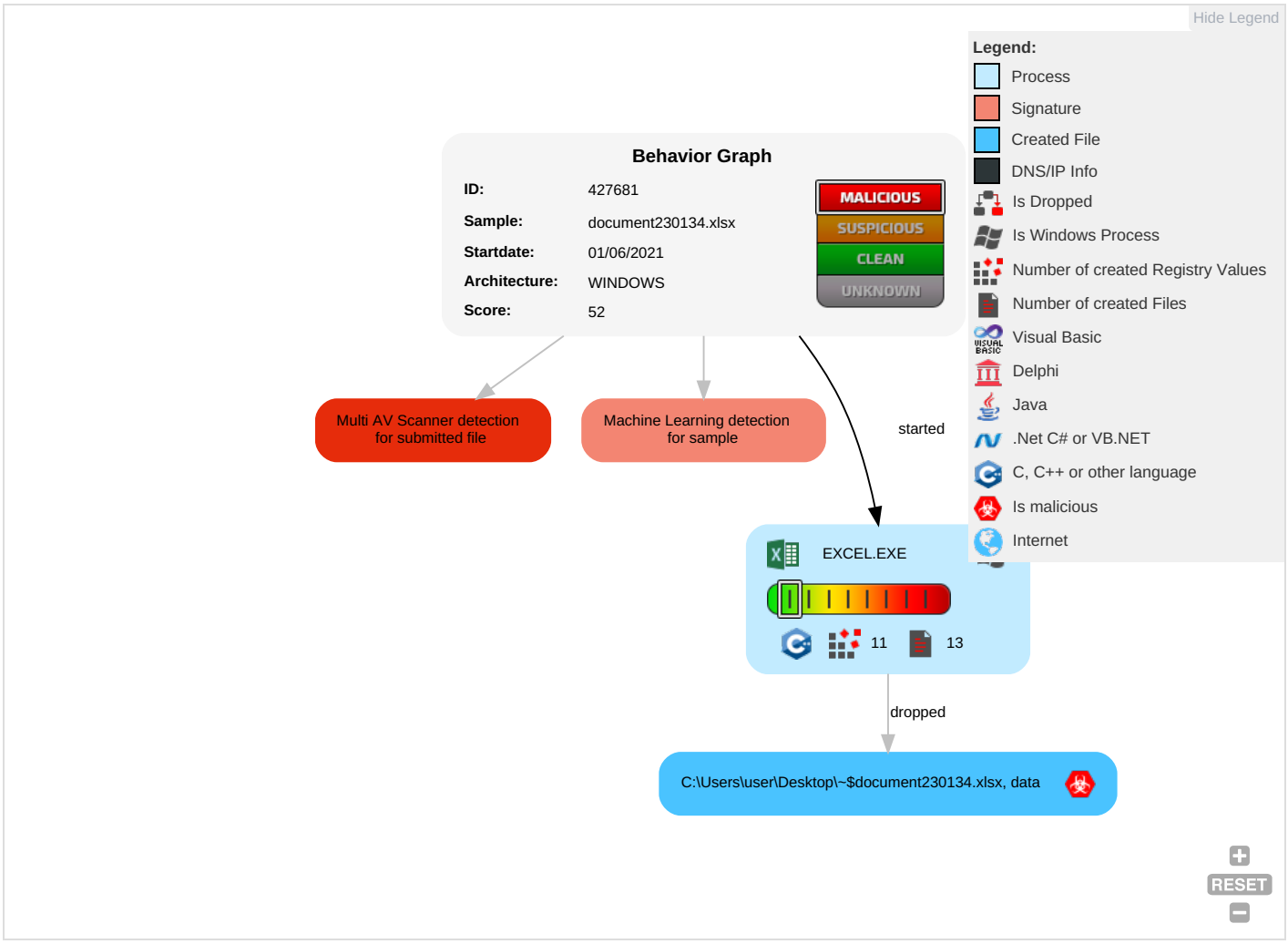
Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

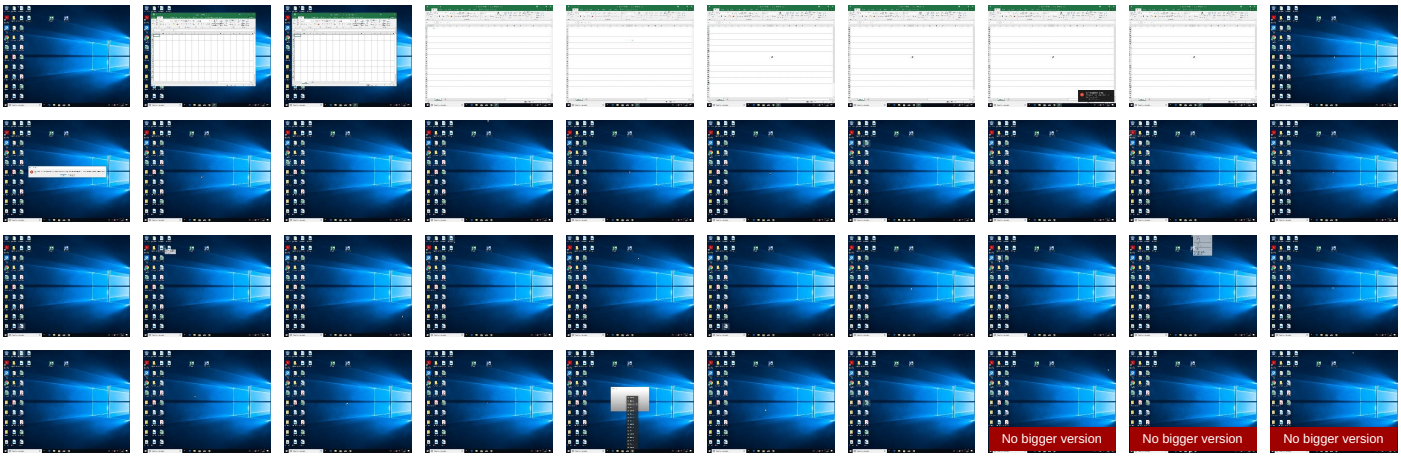
Behavior Graph

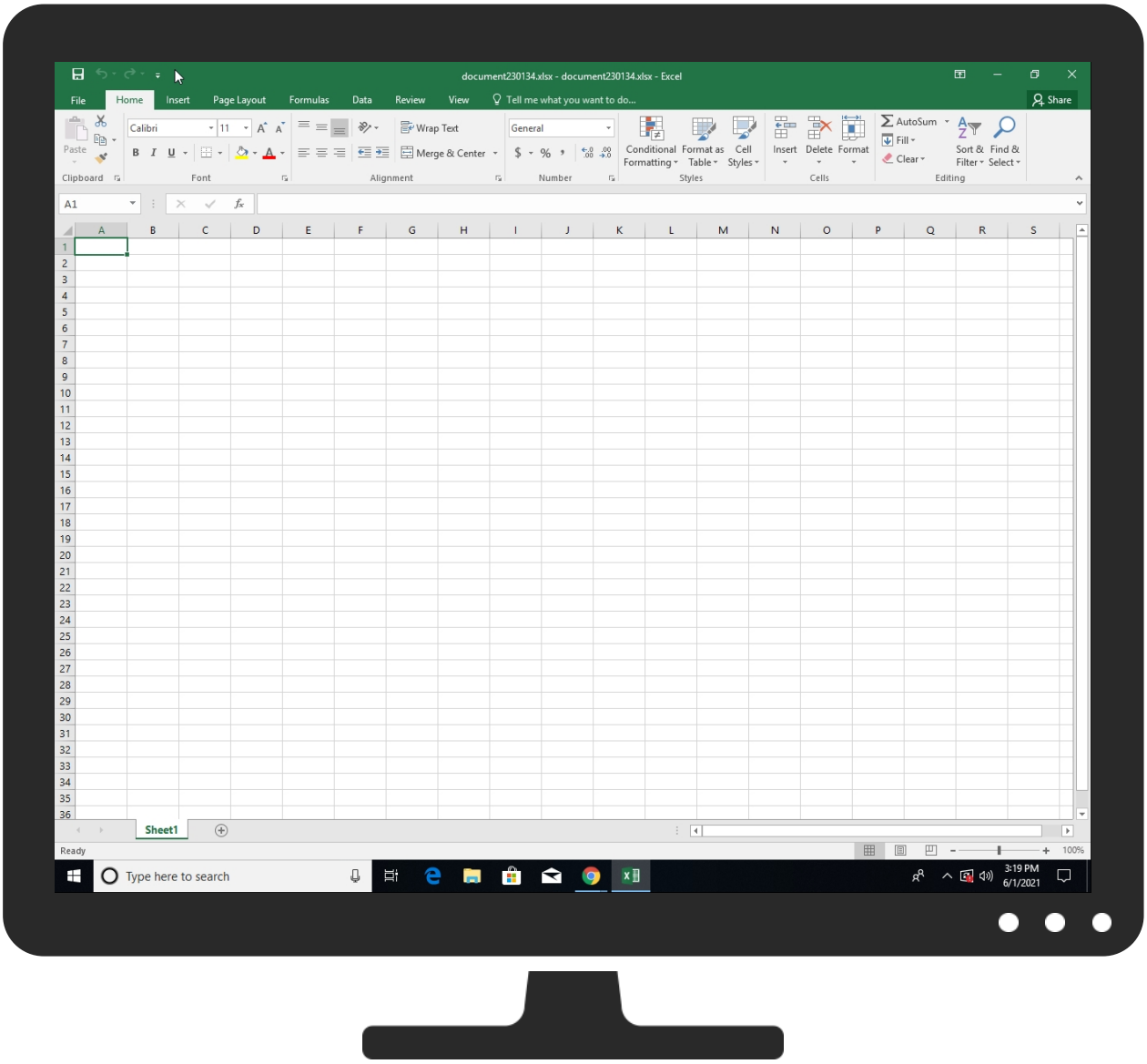


Screenshots

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
document230134.xlsx	53%	Virustotal		Browse
document230134.xlsx	23%	Metadefender		Browse
document230134.xlsx	47%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	
document230134.xlsx	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	427681
Start date:	01.06.2021
Start time:	15:17:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document230134.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	22
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:	mal52.winXLSX@1/1@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe • Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\~$document230134.xlsx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.99766702069879
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	document230134.xlsx
File size:	700955

General

MD5:	badd03190784a6b9d067f2f7ff309a20
SHA1:	5bb5f2ca6419e2ec079d3b24f708f393a431196a
SHA256:	16b1d0cbb8eb4804ccedaed0abd454606f0d237abe3d4f8ac212ff3a027270c7
SHA512:	f57c35895fb9dfd467dfb0f2dd7267454318e18bf6b059e959e59a64715571b865ee064e452deb49c67ee510da97fa9b89af5c8ce0e094672eecf24c4f360312
SSDEEP:	12288:f1zpUhqcwOnuNy0CezOCi0akxpcBDX+gPPJ+GaEj/b5INqKMq7hS5KC:fUhqvOuNy0Cx0HQDuYJJau/bKy6w0C
File Content Preview:	PK.....8Q.R....~...Z.....[Content_Types].xmlUT.....`...`...`..MO.1...&..M..-..cX8.^L.D=x,...n.t.....|..l.;...t..NoU.l..m..h.-....X?)...c.VdH.....B..E.{~.y]G.....1%.wR..B.0..<G.!..5MdTz.& /Z....'....Ct;}.....a..7.$p(..Mb.*...Y...r../J.....

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/427681/sample/document230134.xlsx"

Indicators

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

Summary

Author:	GREEN
Last Saved By:	GREEN
Create Time:	2021-02-03T07:57:22Z
Last Saved Time:	2021-02-03T07:57:35Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	15.0300

Streams

Stream Path: \x1olE10NaTive, File Type: data, Stream Size: 953617

General	
Stream Path:	\x1olE10NaTive
File Type:	data
Stream Size:	953617
Entropy:	6.02549040532
Base64 Encoded:	False

General	
Data ASCII:	. . . . . Y . . . . o . , ... ` . . / . M . . ) . O . . . . . 6 U . . . . . 2 . . G . . . . . _ . . . B . R . . . 2 . h . l . 4 . . . 3 . . . . . B . . . . d . . . f - . . . Z ? 8 . . . . . m . A K . Y . R ^ . f . . . . ? T . . ` u . . . . F . . ` . . 4 n . . . . . ~ . . . 5 p . . . . . p @ . . . l `) . e J . . _ . l . . d 6 . . (u . . . . . S . . . . > . . . p < . . . Q J . y . c . z . P . . . . . < . F M . 4 ! . . h q . . . I k . . . X % . 8 . , : . F . . . . . X [
Data Raw:	bc 10 08 02 03 fd eb b2 59 9c 01 08 ef 6f bd 2c bf 89 d0 81 c5 60 fe bb 2f 8b 4d b0 8b 29 be 4f 98 b9 ff f7 d6 8b 36 55 ff d6 05 14 05 32 1d 05 47 14 ce e2 ff e0 dd 84 5f 9f aa ad 42 00 52 a1 0c 80 32 c1 13 68 de 6c bf 34 80 c8 ae 33 0d 01 d0 97 1c 1c fd 82 b7 42 dc 16 de 04 64 fa 07 f4 66 2d e6 9c 0d 5a 3f 38 9e b0 f1 ae 83 6d ae 41 4b f3 59 d3 52 5e a7 66 a5 b7 ff f4 3f 54 06 82

Stream Path: 94Zni13, File Type: empty, Stream Size: 0

General	
Stream Path:	94Zni13
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 3636 Parent PID: 792

General

Start time:	15:18:51
Start date:	01/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xa90000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$document230134.xlsx	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	BF51E4	WriteFile
C:\Users\user\Desktop\~$document230134.xlsx	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	BF5241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	B020F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	B0211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	B0213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	B0213B	RegSetValueExW

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

Disassembly