

JOeSandbox Cloud BASIC



ID: 509333

Sample Name:

aaaaaaaaaaaa.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 12:24:29

Date: 26/10/2021

Version: 33.0.0 White Diamond

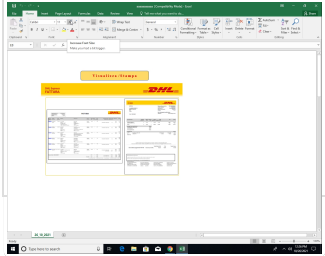
Table of Contents

Table of Contents	2
Windows Analysis Report aaaaaaaaaa.xls	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	3
E-Banking Fraud:	4
System Summary:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
URLs from Memory and Binaries	6
Contacted IPs	6
Public	6
Private	6
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static OLE Info	9
General	9
OLE File "aaaaaaaaa.xls"	9
Indicators	9
Summary	9
Document Summary	9
Streams with VBA	9
Streams	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	9
Analysis Process: EXCEL.EXE PID: 6016 Parent PID: 800	10
General	10
File Activities	10
File Created	10
File Deleted	10
Registry Activities	10
Key Created	10
Key Value Created	10
Disassembly	10
Code Analysis	10

Windows Analysis Report aaaaaaaaaaaaa.xls

Overview

General Information

Sample Name:	aaaaaaaaaaaa.xls
Analysis ID:	509333
MD5:	a8ca4b1a0ab594..
SHA1:	2e8c2f19a0a5875.
SHA256:	9cb3b49716b637..
Tags:	xls
Infos:	
Most interesting Screenshot:	
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

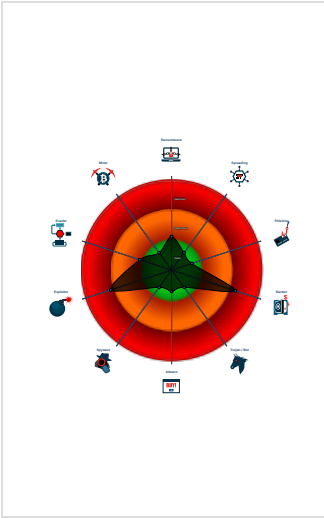
Ursnif Dropper

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

Signatures

- Found detection on Joe Sandbox Clo...
- Multi AV Scanner detection for subm...
- Detected Italy targeted Ursnif droppe...
- Document contains an embedded VB...
- Document contains embedded VBA ...

Classification



Process Tree

- System is w10x64
-  EXCEL.EXE (PID: 6016 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

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

E-Banking Fraud:



Detected Italy targeted Ursnif dropper document

System Summary:



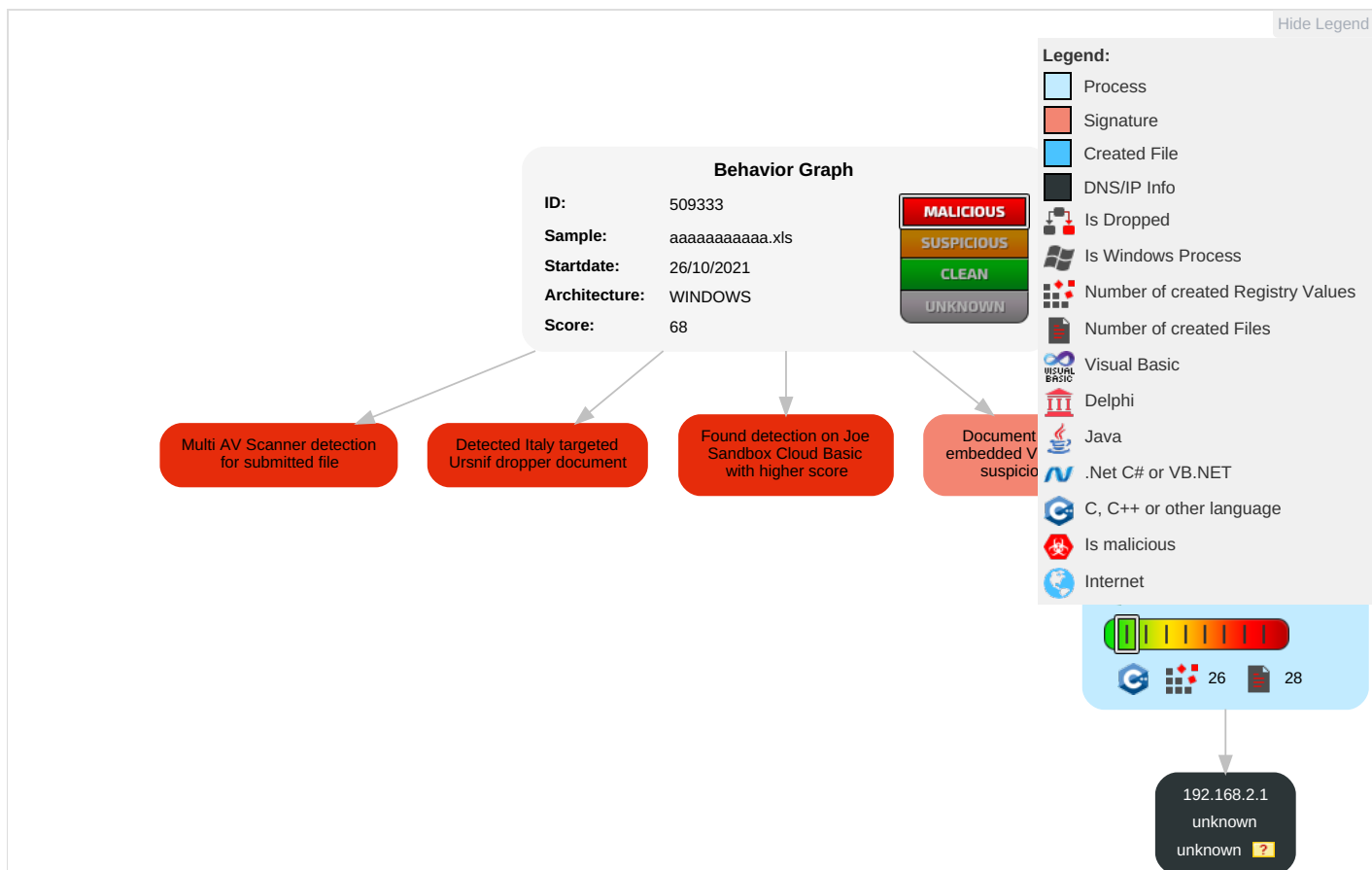
Found detection on Joe Sandbox Cloud Basic with higher score

Document contains an embedded VBA macro with suspicious strings

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	Scripting 1 1	Path Interception	Extra Window Memory Injection 1	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	Malicious System
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Denial of Service
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Denial of Service

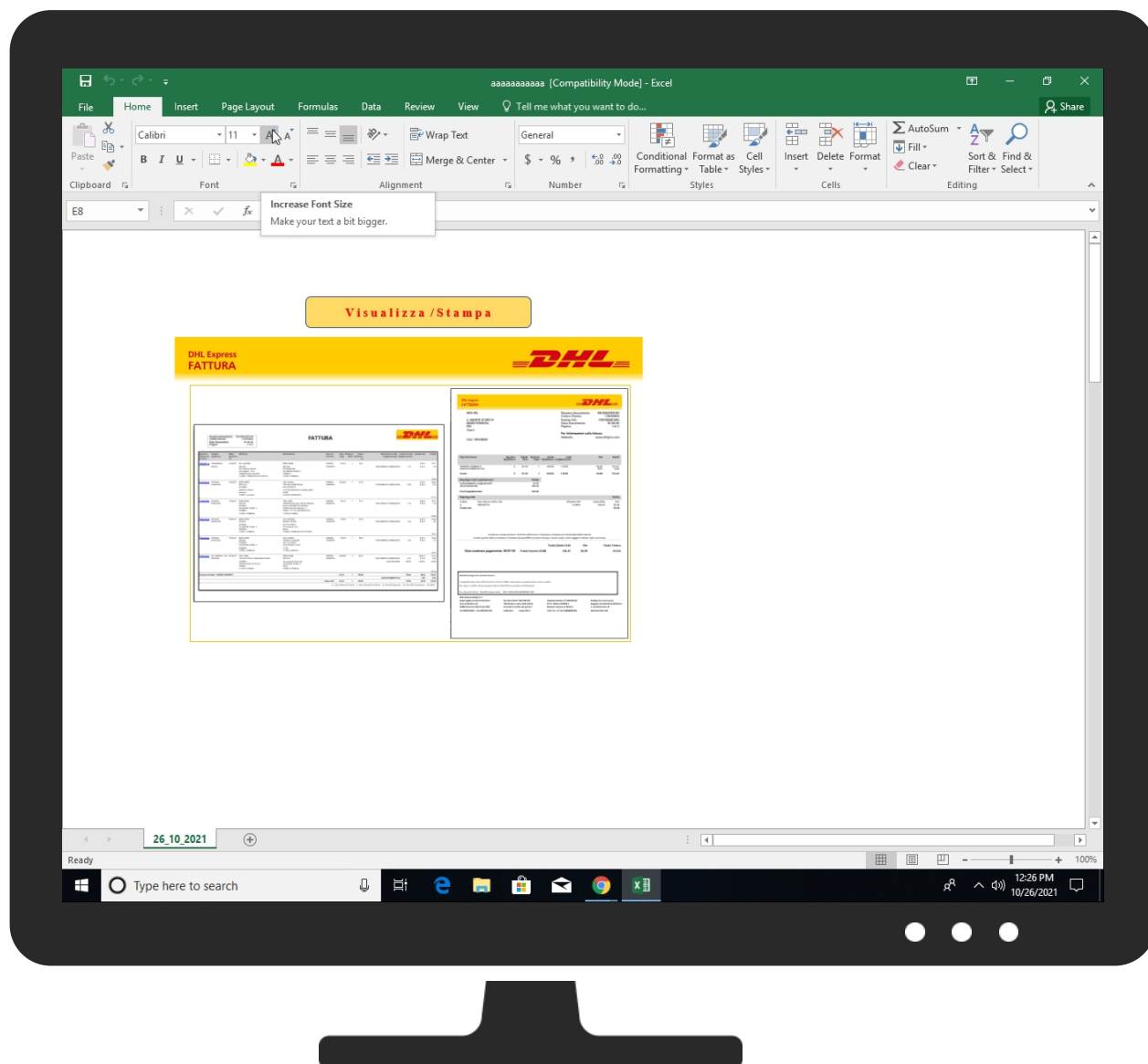
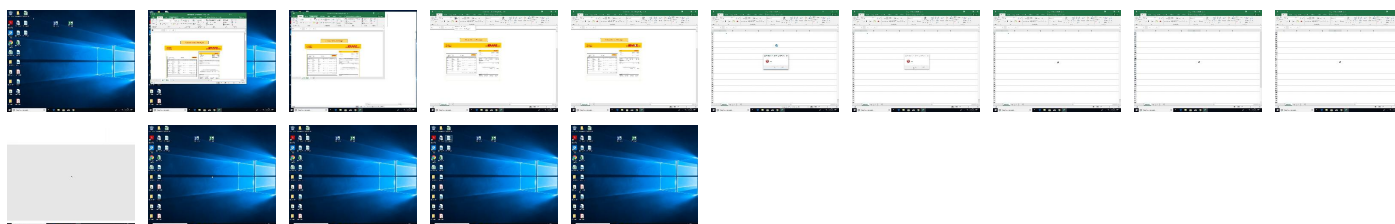
Behavior Graph



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
aaaaa.xls	14%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
----	--------	---------	------	-----	----------	-----------

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	509333
Start date:	26.10.2021
Start time:	12:24:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aaaaaaaaaaa.xls
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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.bank.expl.winXLS@1/1@0/1
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 • Active AutoShape Object • Scroll down • Close Viewer
Warnings:	Show All

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\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4367FA27-1BF9-4B5E-BC42-BFA8671731B4	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	139130
Entropy (8bit):	5.358429083713065
Encrypted:	false
SSDEEP:	1536:DcQlfgxrBdA3gBwfnQ9DQW+zBY34Fi7nXboOidXVE6LWmE9:ZWQ9DQW+zzXaH
MD5:	2E51F9894B5D30F70A63E20B450B437F
SHA1:	47D3E0B8901619E7A3276719AA607716B1A2D7C4
SHA-256:	511F7B2A0593447B25CC55529B34B881FC56132B995034E1E4A87928640FBCFB
SHA-512:	FAD0F769D13490E6435E1899677F0302DCA5B1E6619E0C433A71EC5280805DE7630B69197C22651BFD7C00B17BC39D62FE9B5943CFCAAAE904010D48B33E616
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">..<o:services o:GenerationTime="2021-10-26T10:25:20">..Build: 16.0.14618.30527-->..<o:default>..<o:ticket o:headerName="Authorization" o:headerValue="{}" />..<o:default>..<o:service o:name="Research">..<o:url>https://rr.office.microsoft.com/research/query.aspx<o:url>..</o:service>..<o:service o:name="ORedir">..<o:url>https://o15.officeredir.microsoft.com/r<o:url>..</o:service>..<o:service o:name="ORedirSSL">..<o:url>https://o15.officeredir.microsoft.com/r<o:url>..</o:service>..<o:service o:name="CIViewClientHelpId">..<o:url>https://[MAX.BaseHost]/client/results<o:url>..</o:service>..<o:service o:name="CIViewClientHome">..<o:url>https://[MAX.BaseHost]/client/results<o:url>..</o:service>..<o:service o:name="CIViewClientTemplate">..<o:url>https://ocsa.office.microsoft.com/client/15/help/template<o:url>..</o:service>..<o:

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Create Time/Date: Tue Oct 26 08:18:26 2021, Last Saved Time/Date: Tue Oct 26 08:18:28 2021, Security: 0
Entropy (8bit):	5.783981035047647
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	aaaaaaaaaaa.xls
File size:	56320
MD5:	a8ca4b1a0ab594b286145586e6b4921c
SHA1:	2e8c2f19a0a58755d03bcf12a38e9383d49a8465
SHA256:	9cb3b49716b637ee57db8cc7bd17189ac2fa2489d8ba32a94a7c99f20fa82a5e
SHA512:	42cf117b13e4e972f5565016f92bed73d915dccccb8f7e929ce6850c47dd4befe4dcd8723d6b124fd8f82c5f7da631b54fa4f820b56223b8e41397a73650c6cd
SSDEEP:	1536:FsqIYkElbSkKBEqEXPgsRZmbaoFhZhR0cixIHm0205bQK/6wP6mMCWtmKl:FhYkEluPm3fNRZmbaoFhZhR0cixIHmp
File Content Preview:	>.....F.....

File Icon



Icon Hash:

74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "aaaaaaaaaaa.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
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:	1252
Author:	
Last Saved By:	
Create Time:	2021-10-26 07:18:26.189000
Last Saved Time:	2021-10-26 07:18:28
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6016 Parent PID: 800

General

Start time:	12:25:18
Start date:	26/10/2021
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:	0x3f0000
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

[Show Windows behavior](#)

File Created

File Deleted

Registry Activities

[Show Windows behavior](#)

Key Created

Key Value Created

Disassembly

Code Analysis