**ID:** 321050
**Sample Name:**
sviluppo_economico_18__257.xls
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 10:21:49
**Date:** 20/11/2020
**Version:** 31.0.0 Red Diamond

# Table of Contents

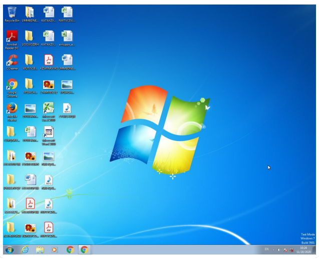
# Analysis Report sviluppo_economico_18__257.xls

## Overview

### General Information

| | |
|---|---|
| Sample Name: | sviluppo_economico_18__257.xls |
| Analysis ID: | 321050 |
| MD5: | 497b53c6668e12.. |
| SHA1: | ae46204ffd41a64.. |
| SHA256: | f07973faea77882.. |

Most interesting Screenshot:



### Detection

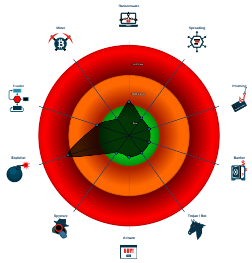
Hidden Macro 4.0

| | |
|---|---|
| Score: | 20 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 80% |

### Signatures

- Yara detected password protected x…
- Unable to load, office file is protecte…

### Classification



## Startup

- System is w7x64
- EXCEL.EXE (PID: 2360 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- cleanup

## Malware Configuration

**No configs have been found**

## Yara Overview

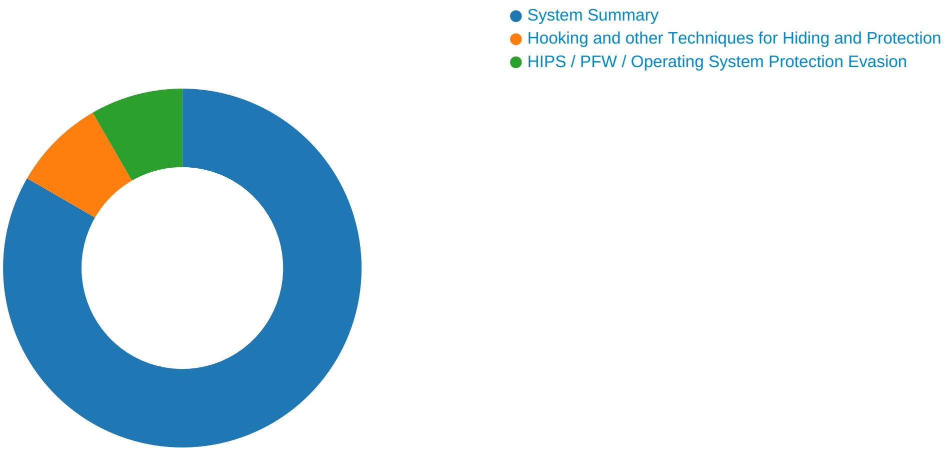
### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| sviluppo_economico_18__257.xls | JoeSecurity_PasswordProtectedXlsWithEmbeddedMacros | Yara detected password protected xls with embedded macros | Joe Security | |

## Sigma Overview

**No Sigma rule has matched**

## Signature Overview



Click to jump to signature section

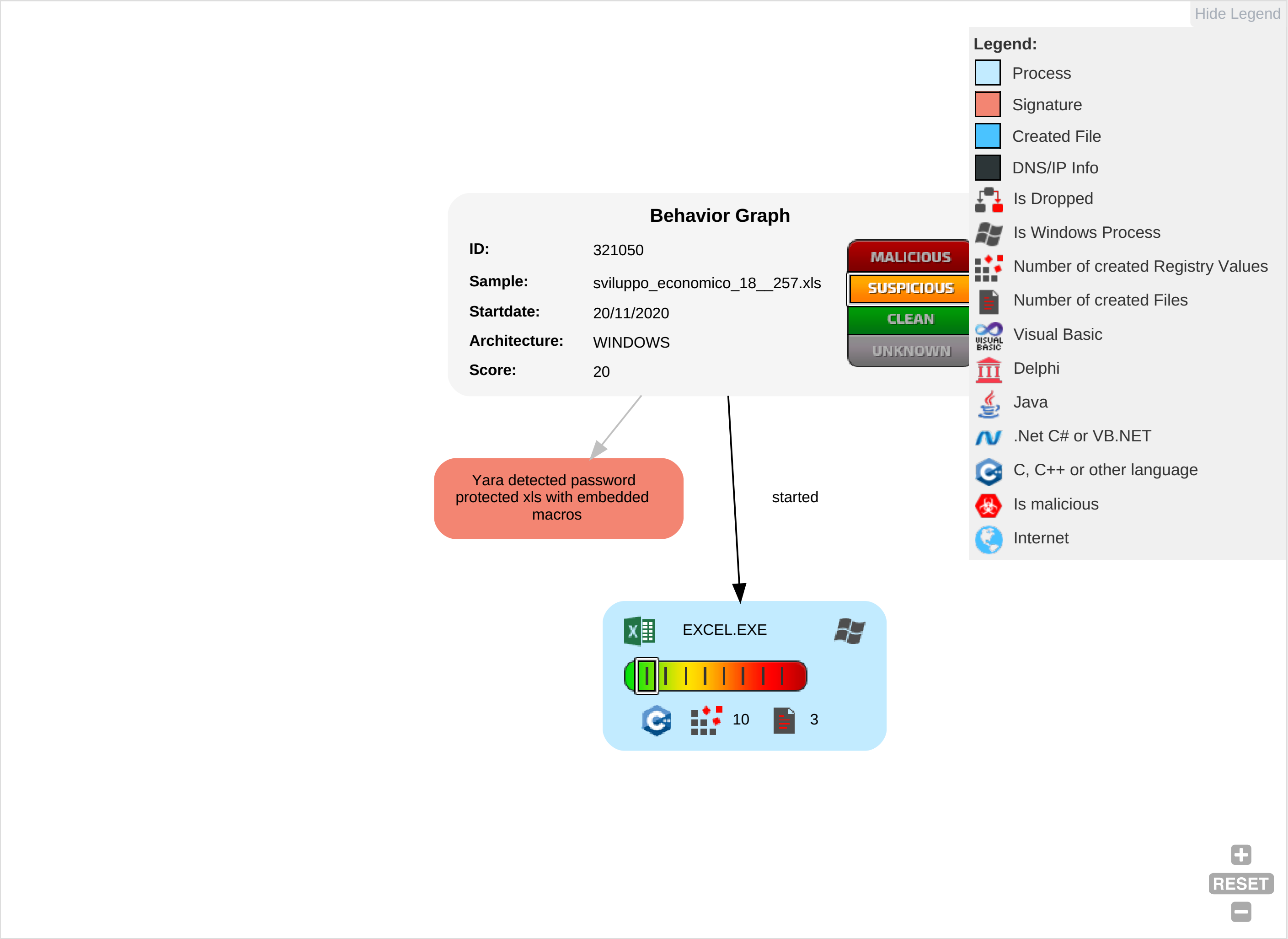
### HIPS / PFW / Operating System Protection Evasion:

**Yara detected password protected xls with embedded macros**

## 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 | Direct Volume Access | 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



**Legend:**

- 🟦 Process
- 🟥 Signature
- 🟦 Created File
- ⬛ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

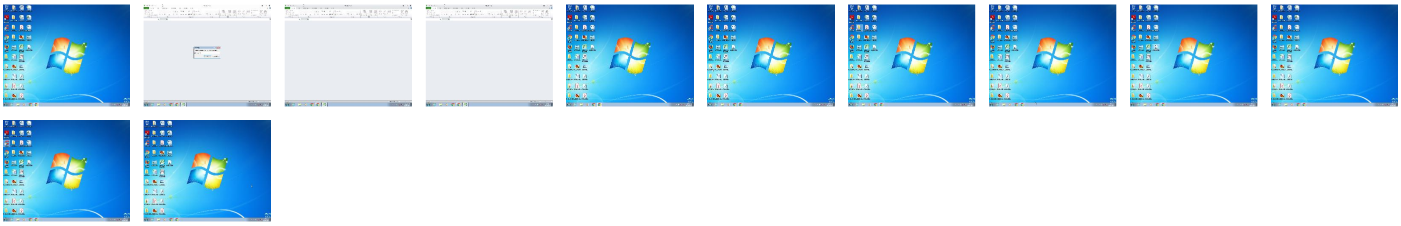
**Behavior Graph**

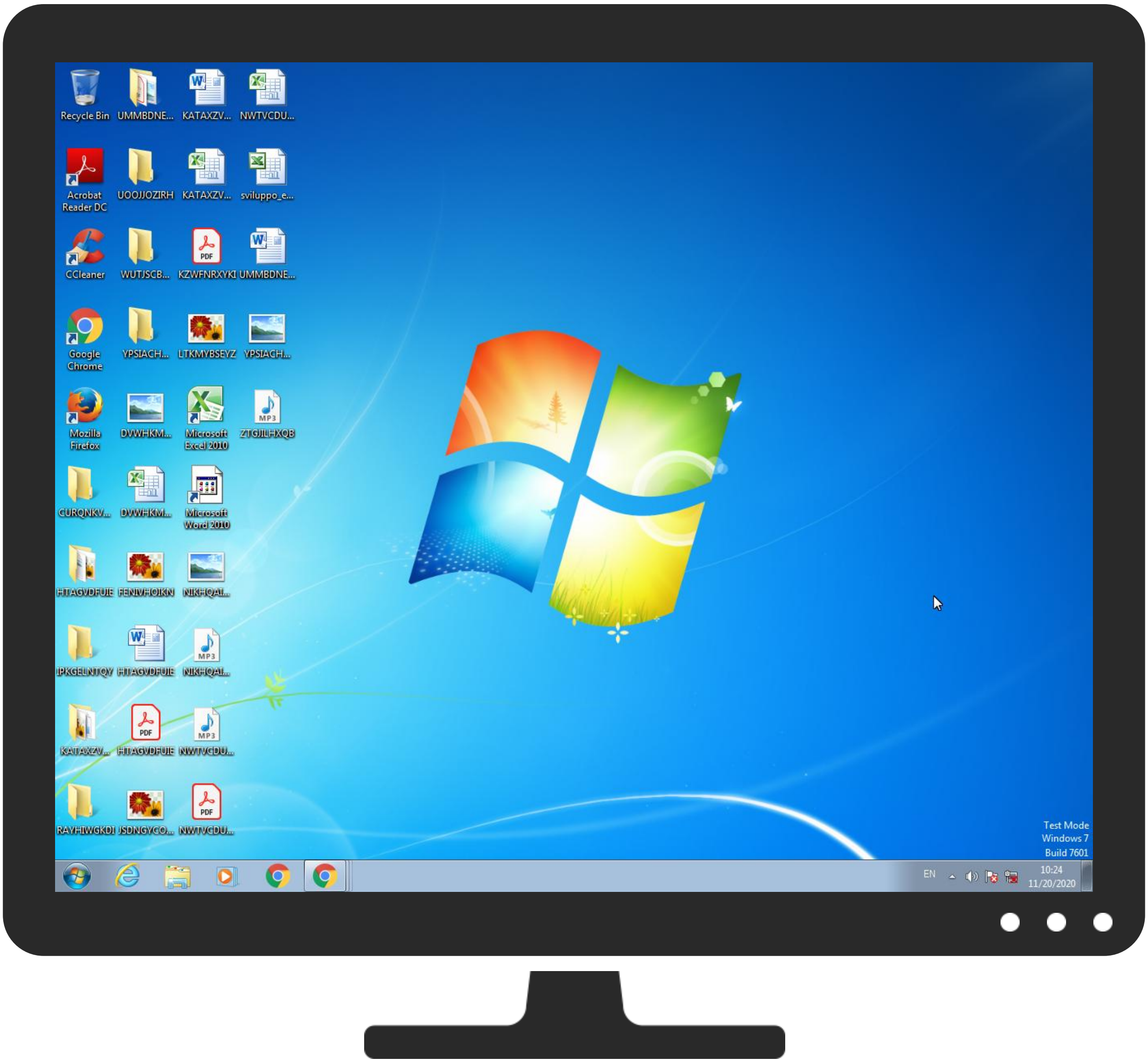
| | |
|---|---|
| **ID:** | 321050 |
| **Sample:** | sviluppo_economico_18__257.xls |
| **Startdate:** | 20/11/2020 |
| **Architecture:** | WINDOWS |
| **Score:** | 20 |

## Screenshots

### Thumbnails

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





# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

**No Antivirus matches**

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

**No Antivirus matches**

## Domains

**No Antivirus matches**

## URLs

**No Antivirus matches**

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted IPs

**No contacted IP infos**

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 31.0.0 Red Diamond |
| Analysis ID: | 321050 |
| Start date: | 20.11.2020 |
| Start time: | 10:21:49 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 3m 56s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | sviluppo_economico_18__257.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: | 2 |
| 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: | • EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | SUS |
| Classification: | sus20.expl.winXLS@1/0@0/0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .xls<br>• Changed system and user locale, location and keyboard layout to Italian - Italy<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All<br>• Exclude process from analysis (whitelisted): dllhost.exe<br>• VT rate limit hit for: /opt/package/joesandbox/database/analysis/321050/sample/sviluppo_economico_18__257.xls |

# 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

**No created / dropped files found**

# Static File Info

## General

| | |
|---|---|
| File type: | Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: veeREfBOcKbNRq, Last Saved By: administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Nov 18 21:59:48 2020, Last Saved Time/Date: Wed Nov 18 22:46:55 2020, Security: 1 |
| Entropy (8bit): | 7.657541825457614 |
| TrID: | • Microsoft Excel sheet (30009/1) 78.94%<br>• Generic OLE2 / Multistream Compound File (8008/1) 21.06% |
| File name: | sviluppo_economico_18__257.xls |
| File size: | 406528 |
| MD5: | 497b53c6668e127364bc30f56555399b |
| SHA1: | ae46204ffd41a649ce4fb9ab24e0add934b68549 |
| SHA256: | f07973faea77882d308d04ea19d66110e3ed3e65c2b8acc<br>45fb6e6fffb5180f4 |
| SHA512: | 92e760cbf9ac4bcbfeecf232b6c4f3dbddf0e7287e9795e4<br>10f68bfea0e0c7e7739d48d5bebab0a1c9e09aa442658c7<br>d406cb586e9dc0f02c0a8227c5f66d1c2 |
| SSDEEP: | 6144:io0aQoiZJoBOKsuHzGNpT6rLh/s7UpT2ETflvilcM<br>SvcseT8O:1wZ6BOKseGNgfa7ET8SvmH |
| File Content Preview: | ......................>............................................................<br>.........................................................................................<br>............................................................................... |

## File Icon

| | |
|---|---|
| | |
| Icon Hash: | e4eea286a4b4bcb4 |

## Static OLE Info

### General

| | |
|---|---|
| Document Type: | OLE |
| Number of OLE Files: | 1 |

### OLE File "sviluppo_economico_18__257.xls"

### Indicators

| | |
|---|---|
| Has Summary Info: | True |
| Application Name: | Microsoft Excel |
| Encrypted Document: | True |
| 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: | False |

### Summary

| | |
|---|---|
| Code Page: | 1252 |
| Author: | veeREfBOcKbNRq |
| Last Saved By: | administrator |
| Create Time: | 2020-11-18 21:59:48 |
| Last Saved Time: | 2020-11-18 22:46:55 |
| Creating Application: | Microsoft Excel |
| Security: | 1 |

### 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

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

| | |
|---|---|
| **General** | |
| Stream Path: | \x5DocumentSummaryInformation |
| File Type: | data |
| Stream Size: | 4096 |
| Entropy: | 0.749350878342 |
| Base64 Encoded: | False |
| Data ASCII: | .......................................+,..0..............P.......X.....<br>.d.......l.......t.......\|................................................<br>..............................................Foglio1.....Foglio2....<br>Foglio3.....Foglio4.....tXClhWqg |
| Data Raw: | fe ff 00 00 0a 00 02 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 0c 02 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 be 01 00 00 |

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

| | |
|---|---|
| **General** | |
| Stream Path: | \x5SummaryInformation |
| File Type: | data |
| Stream Size: | 4096 |
| Entropy: | 0.330245496252 |
| Base64 Encoded: | False |
| Data ASCII: | ................................Oh.....+'..0...............@.......H..<br>...`.......x.........................................veeREfBOcKbNR<br>q..........administrator...........Microsoft Excel.@....b.!....@<br>....Y............................................ |

| General | |
|---|---|
| Data Raw: | fe ff 00 00 0a 00 02 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 b0 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 60 00 00 00 12 00 00 00 78 00 00 00 0c 00 00 00 90 00 00 00 0d 00 00 00 9c 00 00 00 13 00 00 00 a8 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00 |

**Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 393436**

| General | |
|---|---|
| Stream Path: | Workbook |
| File Type: | Applesoft BASIC program data, first line number 16 |
| Stream Size: | 393436 |
| Entropy: | 7.75690503676 |
| Base64 Encoded: | True |
| Data ASCII: | . . . . . . . . Z O . . . . . . . . . . / . . . . . . . . . . . . . ~ . . . . . . . . . . . . h . . . . . . . . . . . . . . . . . . . . . . M .<br>c . r . o . s . o . f . t .  . E . n . h . a . n . c . e . d .  . C . r . y . p . t . o . g . r . a . p . h . i . c .  . P .<br>r . o . v . i . d . e . r .  . v . 1 . . . 0 . . . . . . . % . . . C . . P . . . . . h ; ~ . < ) . X . . . 9 . , # . . . . . . . . .<br>v / . 4 . . . . . . . . . . y . . I . . . . . . . . . . . . . . . . . \\ . p . 5 . R . B @ . . . . . . |
| Data Raw: | 09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 2f 00 c8 00 01 00 04 00 02 00 0c 00 00 00 7e 00 00 00 0c 00 00 00 00 00 00 00 01 68 00 00 04 80 00 00 80 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 |

## Network Behavior

**No network behavior found**

## Code Manipulations

## Statistics

## System Behavior

### Analysis Process: EXCEL.EXE PID: 2360 Parent PID: 584

**General**

| | |
|---|---|
| Start time: | 10:22:45 |
| Start date: | 20/11/2020 |
| 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: | 0x13fcb0000 |
| 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 Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|

### Registry Activities

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|

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

## Disassembly