
**ID:** 528761
**Sample Name:** sample2.xls.vir
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 18:41:48
**Date:** 25/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

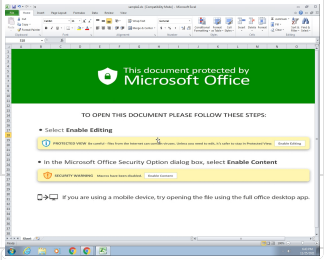
# Windows Analysis Report sample2.xls.vir

## Overview

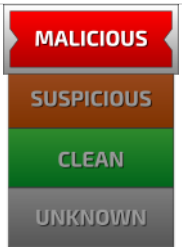
### General Information

| | |
|---|---|
| Sample Name: | sample2.xls.vir (renamed file extension from vir to xls) |
| Analysis ID: | 528761 |
| MD5: | 75c10281f9cae79.. |
| SHA1: | 7bd8c6de6d714ff.. |
| SHA256: | 53a57594efe3312. |
| Tags: | vir xlsx |
| Infos: | |

Most interesting Screenshot:




### Detection



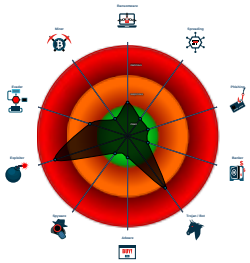

Hidden Macro 4.0

| | |
|---|---|
| Score: | 88 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Performs DNS queries to domains w…
- Office document connecting to susp…
- Potential document exploit detected…
- Yara signature match
- Found a hidden Excel 4.0 Macro she…

### Classification



## Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2644 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2256 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2568 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test1.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 3000 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\test2.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

### Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| sample2.xls.xls | SUSP_Excel4Macro_AutoOpen | Detects Excel4 macro use with auto open / close | John Lambert @JohnLaTwC | • 0x0:$header_docf: D0 CF 11 E0<br>• 0x124c8:$s1: Excel<br>• 0x1358c:$s1: Excel<br>• 0x34b5:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A |
| sample2.xls.xls | JoeSecurity_XlsWithMacro4 | Yara detected Xls With Macro 4.0 | Joe Security | |
| sample2.xls.xls | JoeSecurity_HiddenMacro | Yara detected hidden Macro 4.0 in Excel | Joe Security | |

### Dropped Files

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| C:\Users\user\Desktop\sample2.xls.xls | SUSP_Excel4Macro_AutoOpen | Detects Excel4 macro use with auto open / close | John Lambert @JohnLaTwC | • 0x0:$header_docf: D0 CF 11 E0<br>• 0x124c8:$s1: Excel<br>• 0x1358c:$s1: Excel<br>• 0x34b5:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 01 3A |
| C:\Users\user\Desktop\sample2.xls.xls | JoeSecurity_XlsWithMacro4 | Yara detected Xls With Macro 4.0 | Joe Security | |
| C:\Users\user\Desktop\sample2.xls.xls | JoeSecurity_HiddenMacro | Yara detected hidden Macro 4.0 in Excel | Joe Security | |

## Sigma Overview

### System Summary:

**Sigma detected: Regsvr32 Command Line Without DLL**

**Sigma detected: Microsoft Office Product Spawning Windows Shell**

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

**Multi AV Scanner detection for submitted file**

### Software Vulnerabilities:

**Document exploit detected (process start blacklist hit)**

**Document exploit detected (UrlDownloadToFile)**

**Potential document exploit detected (performs DNS queries with low reputation score)**

### Networking:

**Performs DNS queries to domains with low reputation**

**Office document connecting to suspicious TLD**

### System Summary:

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

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

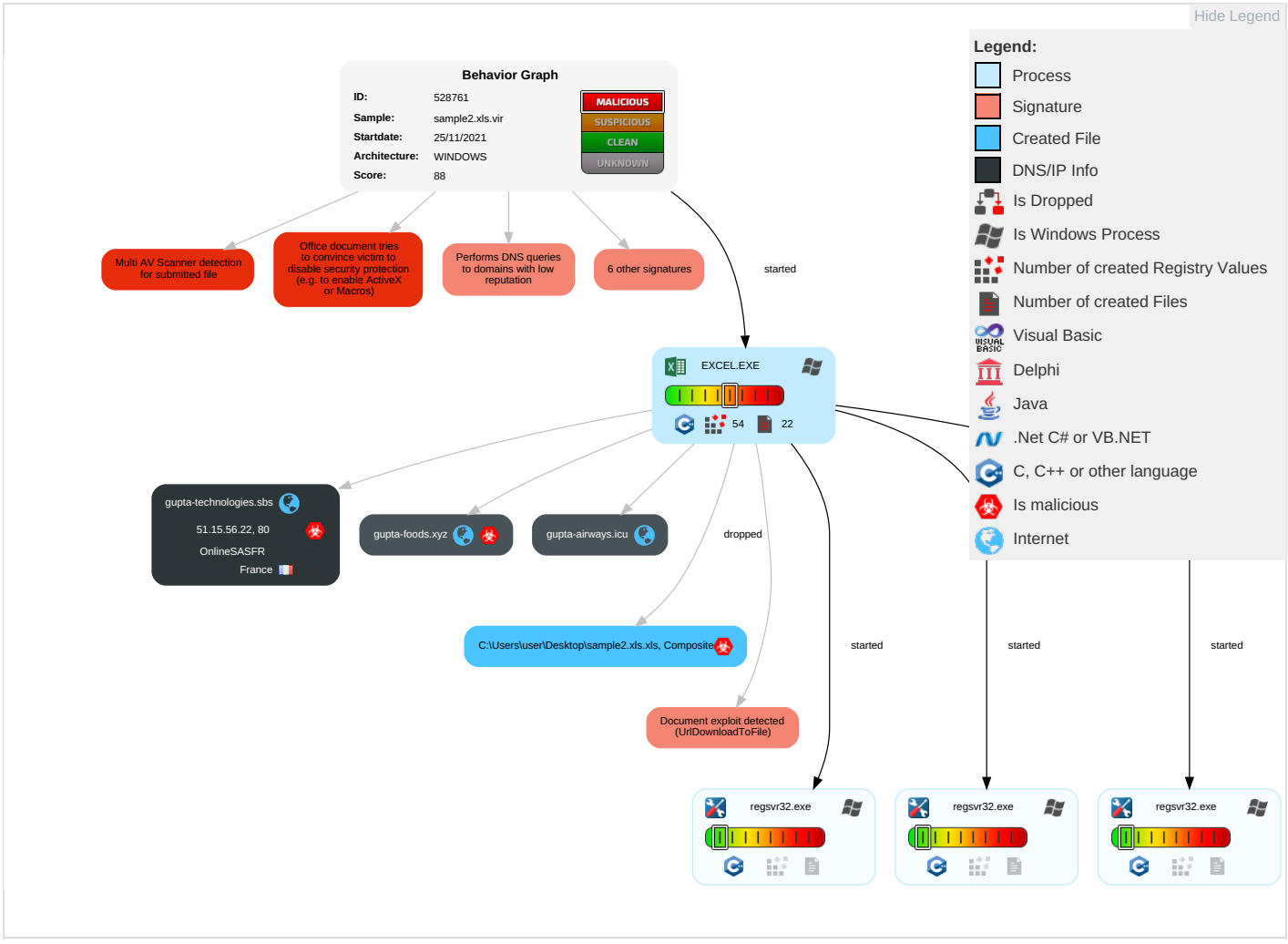
**Yara detected hidden Macro 4.0 in Excel**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | R S E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scripting 1 | Path Interception | Process Injection 1 | Disable or Modify Tools 1 | OS Credential Dumping | Virtualization/Sandbox Evasion 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Non-Application Layer Protocol 1 | Eavesdrop on Insecure Network Communication | R T W A |
| Default Accounts | Exploitation for Client Execution 3 2 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 | LSASS Memory | File and Directory Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Application Layer Protocol 1 | Exploit SS7 to Redirect Phone Calls/SMS | R W W A |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 | Security Account Manager | System Information Discovery 2 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Steganography | Exploit SS7 to Track Device Location | C D C B |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Scripting 1 | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | |

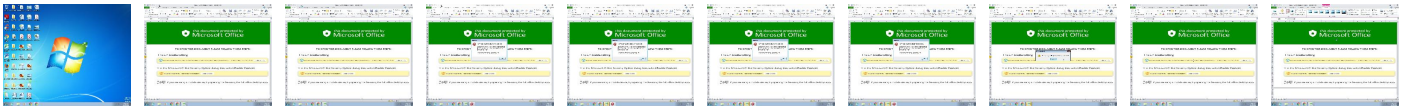
## Behavior Graph

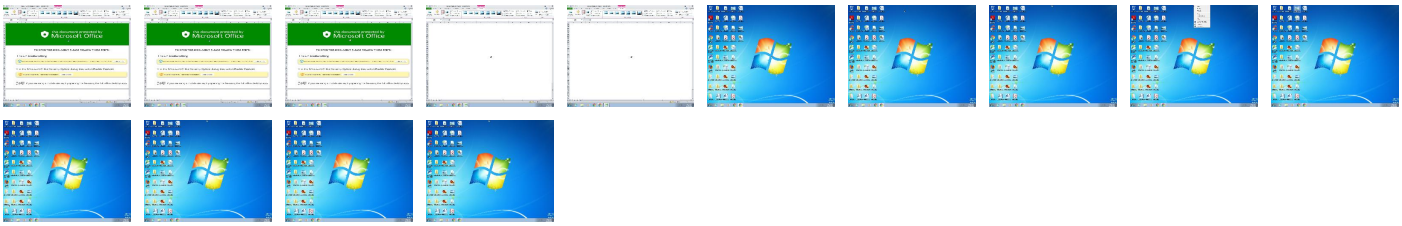


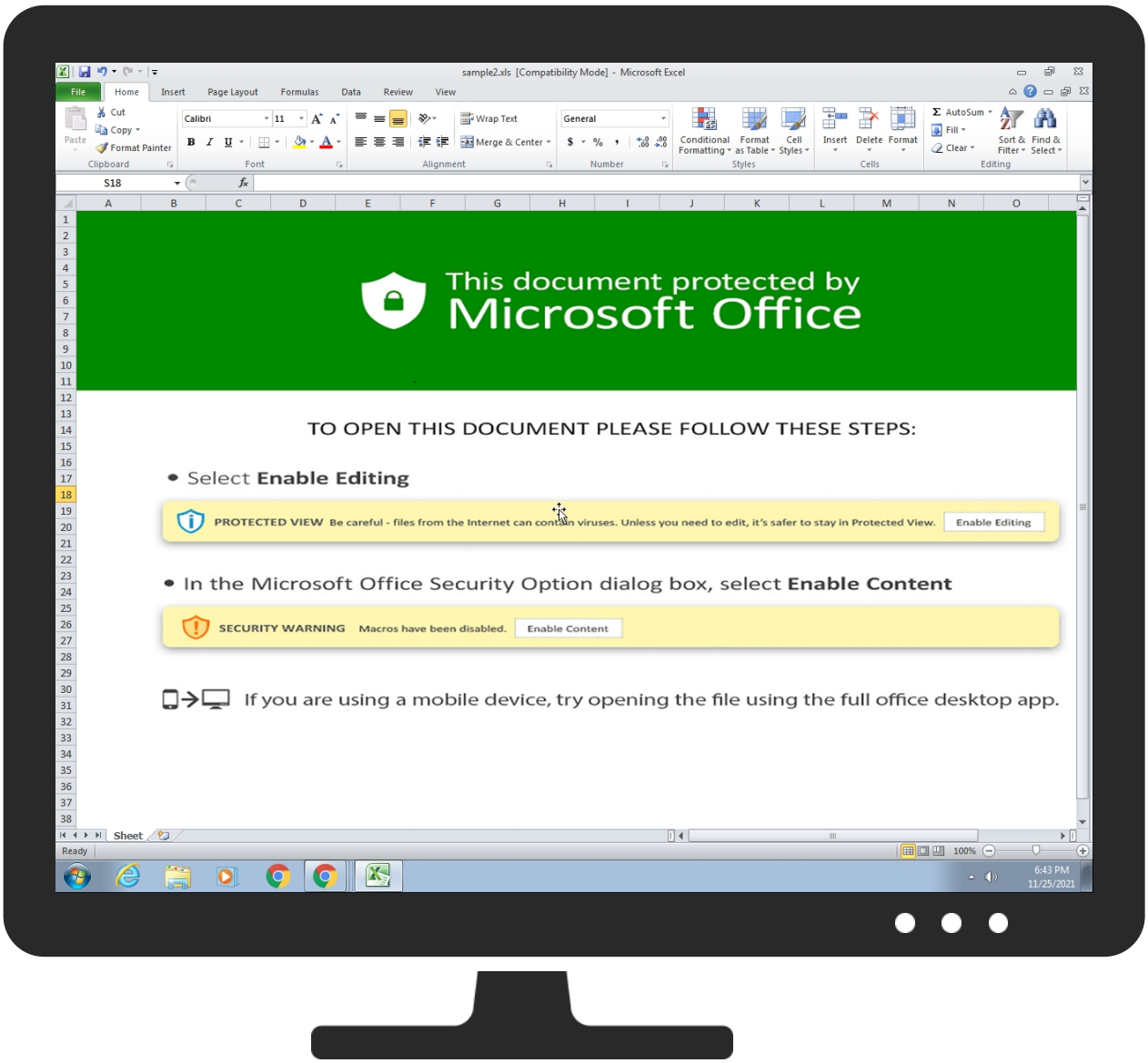

## Screenshots

### 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 |
|---|---|---|---|---|
| sample2.xls.xls | 37% | Virustotal | | Browse |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

| No Antivirus matches |
|---|

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.%s.comPA | 0% | URL Reputation | safe | |
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | 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 |
|---|---|---|---|---|---|
| gupta-foods.xyz | 51.15.56.22 | true | true | | unknown |
| gupta-airways.icu | 51.15.56.22 | true | false | | unknown |
| gupta-technologies.sbs | 51.15.56.22 | true | false | | unknown |

### URLs from Memory and Binaries

### Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 51.15.56.22 | gupta-foods.xyz | France | | 12876 | OnlineSASFR | true |

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 528761 |
| Start date: | 25.11.2021 |
| Start time: | 18:41:48 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 7m 20s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | sample2.xls.vir (renamed file extension from vir to xls) |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP1 (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: | 8 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal88.troj.expl.winXLS@7/4@3/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |

| | |
|---|---|
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<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 |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 18:43:26 | API Interceptor | 199x Sleep call for process: regsvr32.exe modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| OnlineSASFR | EzCOXP6oxy.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | IkroV40UrZ.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | C1Q17Dg4RT.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | MakbLShaqA.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | MakbLShaqA.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | tUJXpPwU27.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | pYebrdRKvR.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | pPX9DaPVYj.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | wUKXjICs5f.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | cRC6TZG6Wx.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | qrb6jVwzoe.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | 1711.doc | Get hash | malicious | Browse | • 195.154.146.35 |
| | j9ZfvcmyKN | Get hash | malicious | Browse | • 51.158.220.39 |
| | GQwxmGZFvtg.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | wNjqkrm8pH.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | 5YO8hZg21O.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | dUGnMYeP1C.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | yFAXc9z51V.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | 9fC0as7YLE.dll | Get hash | malicious | Browse | • 195.154.146.35 |
| | FIyE6huzxV.dll | Get hash | malicious | Browse | • 195.154.146.35 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

## Created / dropped Files

| C:\Users\user\AppData\Local\Temp\7D1C.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 1536 |
| Entropy (8bit): | 1.1464700112623651 |
| Encrypted: | false |
| SSDEEP: | 3:YmsaITlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X |
| MD5: | 72F5C05B7EA8DD6059BF59F50B22DF33 |
| SHA1: | D5AF52E129E15E3A34772806F6C5FBF132E7408E |
| SHA-256: | 1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164 |
| SHA-512: | 6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | .....>..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\~DF30EC3661E732423E.TMP | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 28672 |
| Entropy (8bit): | 3.273337417227373 |
| Encrypted: | false |
| SSDEEP: | 768:DPdjpk3hOdsylKlgxopeiBNhZFGzE+cL2kdAJJ6Q470:5Nk3hOdsylKlgxopeiBNhZFGzE+cL2ko |
| MD5: | D5179EC42D940F87860096C6723AB54D |
| SHA1: | B382B6F7D9FAE38B8A0D1C13B790B216B85A92C0 |
| SHA-256: | 11BD2AD09C3D35E05FE908B1CF17ABC875E95DEBCCCC821204BFDDE8AE2A411D |
| SHA-512: | 92559C475C1818BEF833FEE331ED65D0D2A9EB40732BF5B97E5F97DF85DF71F045CCC4E4539765A4DEEC4CB1BDCCBA06BB41158F42D7D0BDABDED66AD5BC A174 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Temp\~DF6FA4235239FD3AE0.TMP | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 512 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:: |
| MD5: | BF619EAC0CDF3F68D496EA9344137E8B |
| SHA1: | 5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5 |
| SHA-256: | 076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560 |
| SHA-512: | DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | ..... ..... |

| C:\Users\user\Desktop\sample2.xls.xls | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | Composite Document File V2 Document, Little Endian, Os: MacOS, Version 6.11, Code page: -535, Last Saved By: Microsoft Office User, Name of Creating Application: Microsoft Macintosh Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Sun Nov 21 19:57:52 2021, Security: 0 |

| C:\Users\user\Desktop\sample2.xls.xls | |
|---|---|
| Category: | dropped |
| Size (bytes): | 84480 |
| Entropy (8bit): | 6.340445126312824 |
| Encrypted: | false |
| SSDEEP: | 1536:NNk3hOdsylKlgxopeiBNhZFGzE+cL2kdAy91vrVmxJiME2GhdD52lZPFu1AOg0+Q:Tk3hOdsylKlgxopeiBNhZFGzE+cL2kdj |
| MD5: | F5DF0164EDB6DDBA1741BE8E96278AE7 |
| SHA1: | 98D665DD496C78B7D1490F190196FB92118833E0 |
| SHA-256: | 91B81F22FEB1C6C4BBA109BB19C2D9A6948096D46D5A41B40A40858828AA5CCB |
| SHA-512: | 28F497C9EDFF05E5E696CDB05AF1084ADB41756B113694FDCEA4C493D5C9856C185AD9D7FD9626A0613EC9E22D96D11DDA087AAB7100F5DFF008131745A444<br>0 |
| Malicious: | **true** |
| Yara Hits: | • Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: John Lambert @JohnLaTwC<br>• Rule: JoeSecurity_XlsWithMacro4, Description: Yara detected Xls With Macro 4.0, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: Joe Security<br>• Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\sample2.xls.xls, Author: Joe Security |
| Reputation: | low |
| Preview: | .....>.....<br>.....ZO.....<br>.....\.p....usersoft Office User B.....a.....=. .....=.....p\D8.....X<br>.@.....".....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..... |

# Static File Info

## General

| | |
|---|---|
| File type: | Composite Document File V2 Document, Little Endian, Os: MacOS, Version 6.11, Code page: -535, Last Saved By: Microsoft Office User, Name of Creating Application: Microsoft Macintosh Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Sun Nov 21 19:57:52 2021, Security: 0 |
| Entropy (8bit): | 6.340423482922574 |
| TrID: | • Microsoft Excel sheet (30009/1) 78.94%<br>• Generic OLE2 / Multistream Compound File (8008/1) 21.06% |
| File name: | sample2.xls.xls |
| File size: | 84481 |
| MD5: | 75c10281f9cae799f72d6b949199fd91 |
| SHA1: | 7bd8c6de6d714ff5e0b8f450203d24c8dd30495d |
| SHA256: | 53a57594efe3312565fd5415ad3d7066799f831bb685473<br>7ffaf87fe0119af01 |
| SHA512: | f038bd4f0d0d6108502a761de35d10cb53b7351c18b744b<br>4c9b247bbf10fdc8962fe516f90c1a05a7583731711dcd9<br>8b46a3667a3e9d9f79a48d035fc0e1ba49 |
| SSDEEP: | 1536:oNk3hOdsylKlgxopeiBNhZFGzE+cL2kdAy91vrVm<br>xJiME2GhdD52lZPFu1AOg0+d:wk3hOdsylKlgxopeiBNh<br>ZFGzE+cL2kd0 |
| File Content Preview: | .....>.....<br>.....<br>..... |

## File Icon

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

## Static OLE Info

### General

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

### OLE File "sample2.xls.xls"

### Indicators

| | |
|---|---|
| Has Summary Info: | True |

### Indicators

| | |
|---|---|
| Application Name: | Microsoft Macintosh 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: | -535 |
| Author: | |
| Last Saved By: | Microsoft Office User |
| Create Time: | 2015-06-05 18:19:34 |
| Last Saved Time: | 2021-11-21 19:57:52 |
| Creating Application: | Microsoft Macintosh Excel |
| Security: | 0 |

### Document Summary

| | |
|---|---|
| Document Code Page: | 10000 |
| Thumbnail Scaling Desired: | False |
| Company: | |
| Contains Dirty Links: | False |
| Shared Document: | False |
| Changed Hyperlinks: | False |
| Application Version: | 1048576 |

### Streams

### Macro 4.0 Code

# Network Behavior

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Nov 25, 2021 18:42:42.486798048 CET | 192.168.2.22 | 8.8.8.8 | 0x5ee5 | Standard query (0) | gupta-foods.xyz | A (IP address) | IN (0x0001) |
| Nov 25, 2021 18:43:03.592708111 CET | 192.168.2.22 | 8.8.8.8 | 0x9dfa | Standard query (0) | gupta-technologies.sbs | A (IP address) | IN (0x0001) |
| Nov 25, 2021 18:43:24.698291063 CET | 192.168.2.22 | 8.8.8.8 | 0x88df | Standard query (0) | gupta-airways.icu | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 25, 2021 18:42:42.525017023 CET | 8.8.8.8 | 192.168.2.22 | 0x5ee5 | No error (0) | gupta-foods.xyz | | 51.15.56.22 | A (IP address) | IN (0x0001) |
| Nov 25, 2021 18:43:03.651011944 CET | 8.8.8.8 | 192.168.2.22 | 0x9dfa | No error (0) | gupta-technologies.sbs | | 51.15.56.22 | A (IP address) | IN (0x0001) |

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Nov 25, 2021 18:43:24.758454084 CET | 8.8.8.8 | 192.168.2.22 | 0x88df | No error (0) | gupta-airways.icu | | 51.15.56.22 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

### Analysis Process: EXCEL.EXE PID: 2644 Parent PID: 596

#### General

| | |
|---|---|
| Start time: | 18:42:17 |
| Start date: | 25/11/2021 |
| 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: | 0x13ff90000 |
| File size: | 28253536 bytes |
| MD5 hash: | D53B85E21886D2AF9815C377537BCAC3 |
| 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

File Moved

#### Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

### Analysis Process: regsvr32.exe PID: 2256 Parent PID: 2644

### General

| | |
|---|---|
| Start time: | 18:43:25 |
| Start date: | 25/11/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Windows\System32\regsvr32.exe" C:\Datop\test.test |
| Imagebase: | 0xff590000 |
| File size: | 19456 bytes |
| MD5 hash: | 59BCE9F07985F8A4204F4D6554CFF708 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: regsvr32.exe PID: 2568 Parent PID: 2644

### General

| | |
|---|---|
| Start time: | 18:43:26 |
| Start date: | 25/11/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Windows\System32\regsvr32.exe" C:\Datop\test1.test |
| Imagebase: | 0xff590000 |
| File size: | 19456 bytes |
| MD5 hash: | 59BCE9F07985F8A4204F4D6554CFF708 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

## Analysis Process: regsvr32.exe PID: 3000 Parent PID: 2644

### General

| | |
|---|---|
| Start time: | 18:43:26 |
| Start date: | 25/11/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Windows\System32\regsvr32.exe" C:\Datop\test2.test |
| Imagebase: | 0xff590000 |
| File size: | 19456 bytes |
| MD5 hash: | 59BCE9F07985F8A4204F4D6554CFF708 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

**File Activities** Show Windows behavior

# Disassembly

## Code Analysis