
**ID:** 501226
**Sample Name:** doc-220808714.xls
**Cookbook:** defaultwindowsofficecookbook.jbs
**Time:** 17:12:45
**Date:** 12/10/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

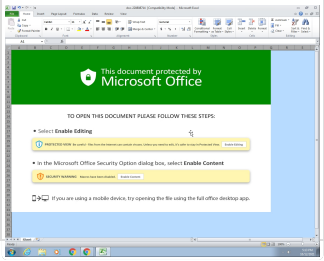
# Windows Analysis Report doc-220808714.xls

## Overview

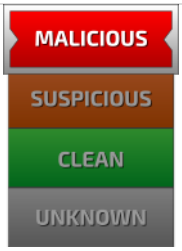
### General Information

| | |
|---|---|
| Sample Name: | doc-220808714.xls |
| Analysis ID: | 501226 |
| MD5: | 2654fdca7197f54.. |
| SHA1: | 149b43a5f8f4d9b.. |
| SHA256: | f5a313c5353ae0d. |
| Infos: | |

Most interesting Screenshot:




### Detection



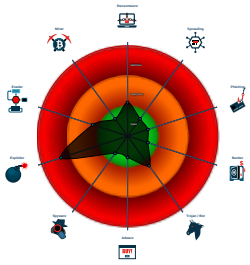

Hidden Macro 4.0

| | |
|---|---|
| Score: | 76 |
| 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…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Document contains embedded VBA …

### Classification



## Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 508 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1212 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1444 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2792 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 |
|---|---|---|---|---|
| doc-220808714.xls | SUSP_Excel4Macro_AutoOpen | Detects Excel4 macro use with auto open / close | John Lambert @JohnLaTwC | • 0x0:$header_docf: D0 CF 11 E0<br>• 0x384aa:$s1: Excel<br>• 0x39557:$s1: Excel<br>• 0x34eb:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A |
| doc-220808714.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)

### System Summary:

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

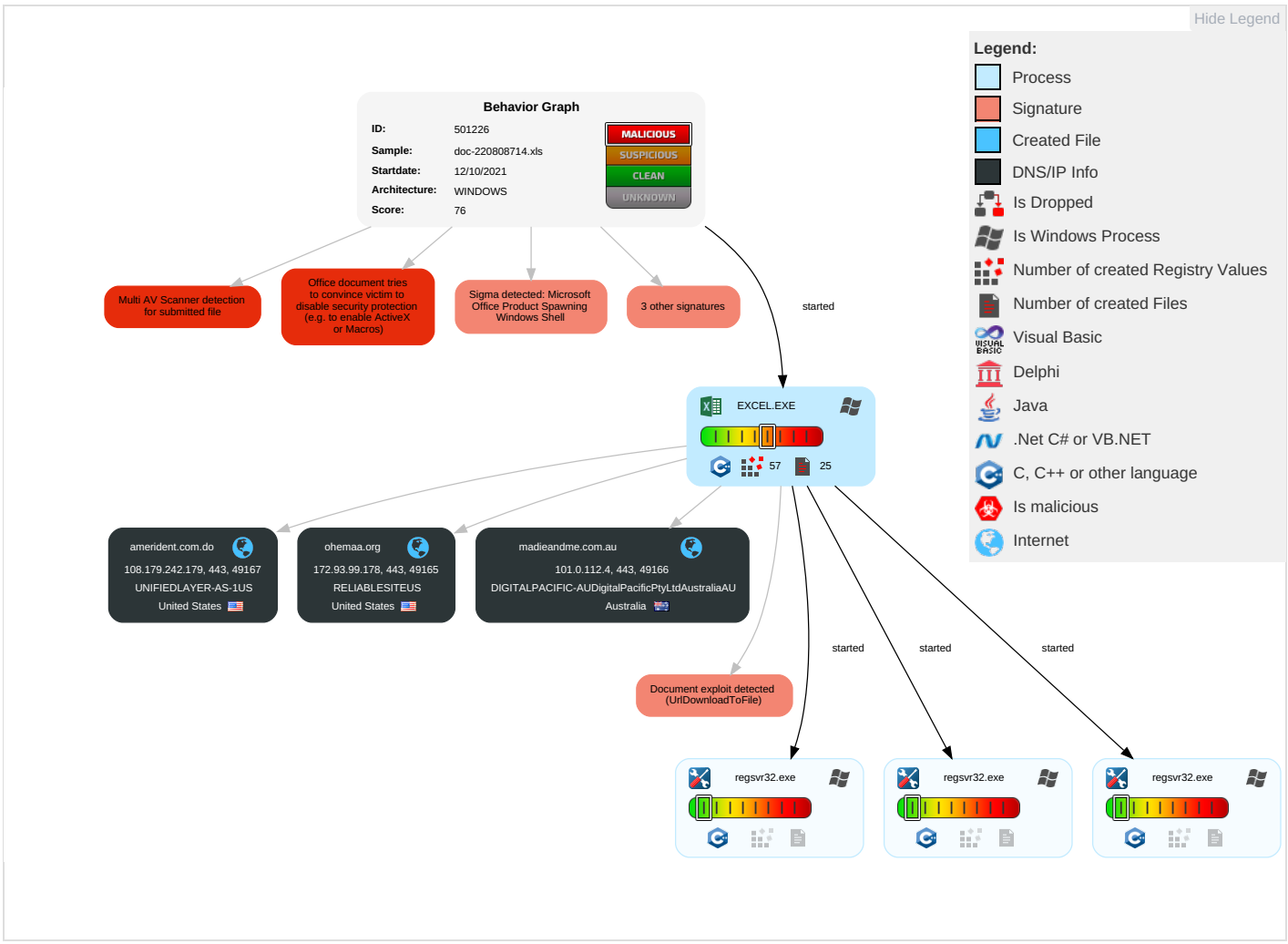
### HIPS / PFW / Operating System Protection Evasion:

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 | Re Se Ef |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Re Tr W Au |
| Default Accounts | Exploitation for Client Execution 2 3 | 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 | Non-Application Layer Protocol 2 | Exploit SS7 to Redirect Phone Calls/SMS | Re W W Au |
| 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 | Application Layer Protocol 1 3 | Exploit SS7 to Track Device Location | Ol De Cl Ba |
| 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 | Ingress Tool Transfer 2 | SIM Card Swap | |

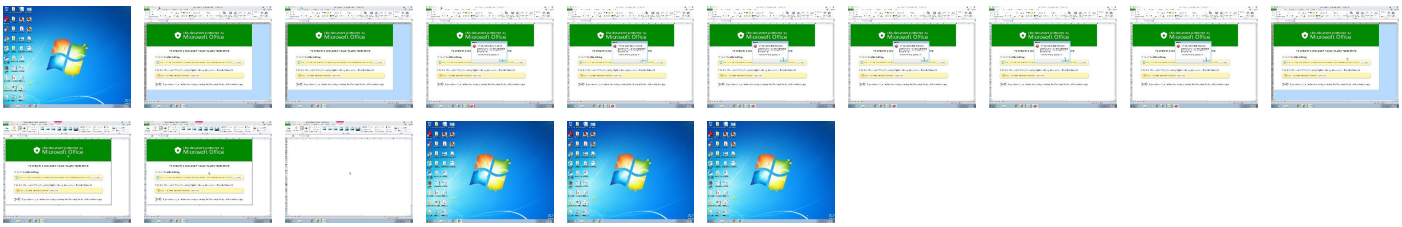
## Behavior Graph

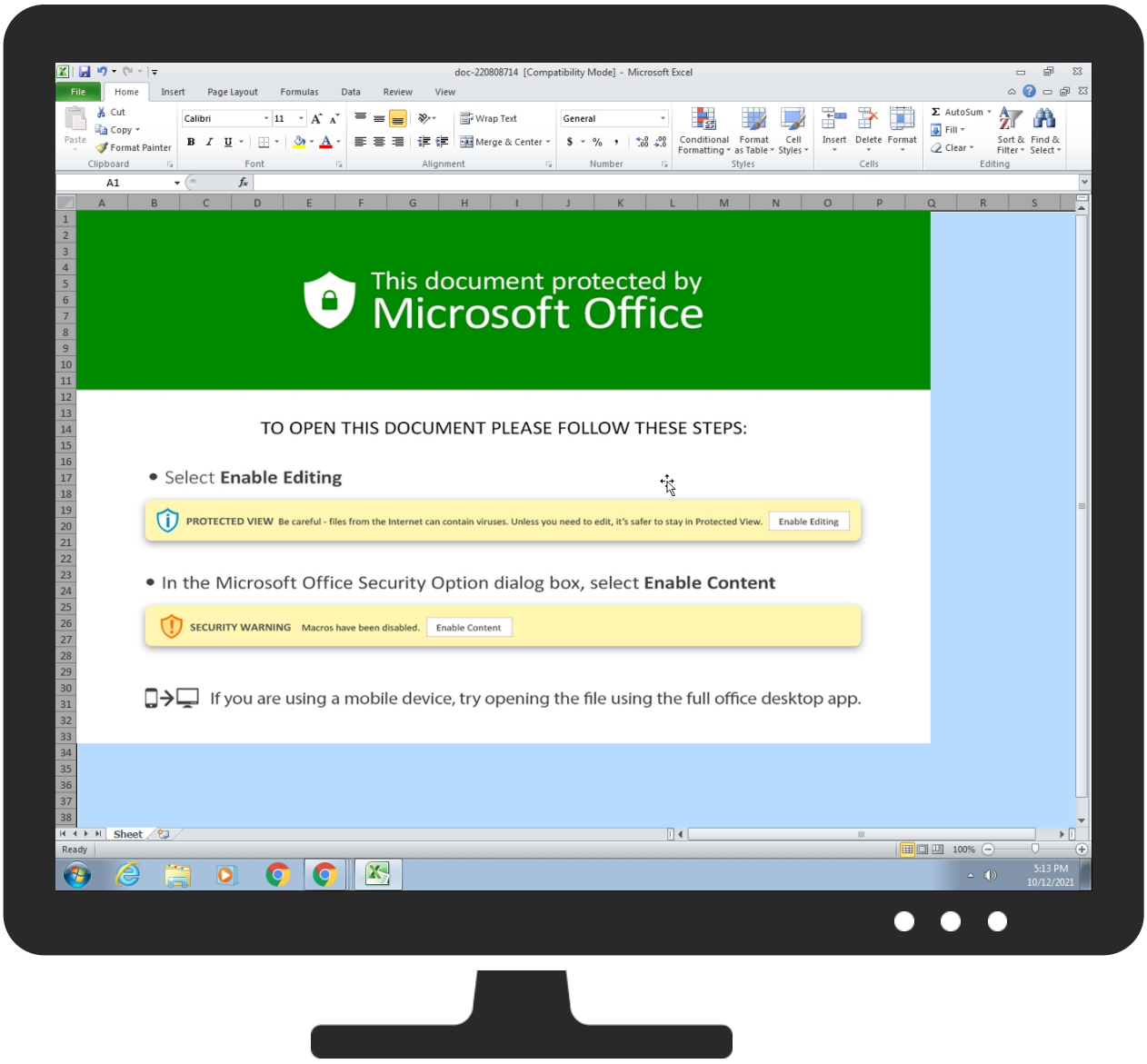



## Screenshots

### 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 |
|---|---|---|---|---|
| doc-220808714.xls | 13% | Virustotal | | Browse |

### Dropped Files

**No Antivirus matches**

### Unpacked PE Files

**No Antivirus matches**

### Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| ohemaa.org | 0% | Virustotal | | Browse |

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://ohemaa.org/HUVm9mDKLW9C/ocrafhh.html | 0% | Avira URL Cloud | safe | |
| http://www.icra.org/vocabulary/. | 0% | URL Reputation | safe | |
| http://https://madieandme.com.au/xnkpOLnvlN6T/ocrafh.html | 0% | Avira URL Cloud | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://www.%s.comPA | 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 | |
| http://https://ameridentcom.do/xdOMlaB0XJ7/ocraf.html | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| ohemaa.org | 172.93.99.178 | true | false | • 0%, Virustotal, Browse | unknown |
| ameridentcom.do | 108.179.242.179 | true | false | | unknown |
| madieandme.com.au | 101.0.112.4 | true | false | | unknown |

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://https://ohemaa.org/HUVm9mDKLW9C/ocrafhh.html | false | • Avira URL Cloud: safe | unknown |
| http://https://madieandme.com.au/xnkpOLnvlN6T/ocrafh.html | false | • Avira URL Cloud: safe | unknown |
| http://https://ameridentcom.do/xdOMlaB0XJ7/ocraf.html | false | • Avira URL Cloud: safe | unknown |

## URLs from Memory and Binaries

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 101.0.112.4 | madieandme.com.au | Australia | | 55803 | DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU | false |
| 108.179.242.179 | ameridentcom.do | United States | | 46606 | UNIFIEDLAYER-AS-1US | false |
| 172.93.99.178 | ohemaa.org | United States | | 23470 | RELIABLESITEUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 501226 |
| Start date: | 12.10.2021 |
| Start time: | 17:12:45 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 46s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | doc-220808714.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: | mal76.expl.winXLS@7/0@3/3 |
| 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 application associated with file extension: .xls<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Found warning dialog<br>• Click Ok<br>• Found warning dialog<br>• Click Ok<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 17:13:29 | API Interceptor | 217x Sleep call for process: regsvr32.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 108.179.242.179 | 414d46ac_by_Libranalysis.xls | Get hash | malicious | Browse | |
| | 414d46ac_by_Libranalysis.xls | Get hash | malicious | Browse | |
| 172.93.99.178 | 430#U0437.js | Get hash | malicious | Browse | • globalawardscheme.com/wp-content/cache/nextend/web/combined/sserv.jpg |
| | 430#U0437.js | Get hash | malicious | Browse | • globalawardscheme.com/wp-content/cache/nextend/web/combined/sserv.jpg |
| | 34029.doc | Get hash | malicious | Browse | • justevolvewithgrace.com/cgi-sys/suspendedpage.cgi |
| | http://51.254.121.123/wp-content/0AR/com/US | Get hash | malicious | Browse | • justevolvewithgrace.com/cgi-sys/suspendedpage.cgi |
| | 8590170.doc | Get hash | malicious | Browse | • justevolvewithgrace.com/cgi-sys/suspendedpage.cgi |

## Domains

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| amerident.com.do | 414d46ac_by_Libranalysis.xls | Get hash | malicious | Browse | • 108.179.242.179 |
| | 414d46ac_by_Libranalysis.xls | Get hash | malicious | Browse | • 108.179.242.179 |

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU | ITT - PPCL-2021-0515-PKG4 - pipping and drilling Services.doc | Get hash | malicious | Browse | • 116.90.56.138 |
| | Inquiry-Doors.exe | Get hash | malicious | Browse | • 101.0.91.38 |
| | product specification.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | 7PUgGUWM2l | Get hash | malicious | Browse | • 182.160.170.135 |
| | Attached Quotation.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | Cd9EA600XXdm0tl.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | E8ljMuBj9L | Get hash | malicious | Browse | • 111.67.13.18 |
| | QcXQmNSaSp | Get hash | malicious | Browse | • 49.156.27.62 |
| | arm7 | Get hash | malicious | Browse | • 111.67.13.28 |
| | QYUNlRkkn1.exe | Get hash | malicious | Browse | • 203.16.60.34 |
| | 6Y5P9BoimMLclbt.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | gunzipped.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | SecuriteInfo.com.Variant.Bulz.627351.21436.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | ENQUIRY.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | 16wKmiVoPj05ynr.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | PURCHASE ORDER.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | PO.NO.V21015.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | New Inquiry 21411JA20pdf.exe | Get hash | malicious | Browse | • 101.0.117.102 |
| | fsd8ks3VNb.exe | Get hash | malicious | Browse | • 101.0.105.170 |
| | y1FOl1vVPA.exe | Get hash | malicious | Browse | • 101.0.86.146 |
| UNIFIEDLAYER-AS-1US | jjBv8SpZXm.exe | Get hash | malicious | Browse | • 192.185.0.218 |
| | Scan_0978.exe | Get hash | malicious | Browse | • 173.254.94.114 |
| | pKD3j672HL.exe | Get hash | malicious | Browse | • 192.185.131.113 |
| | heiedrNhQ8 | Get hash | malicious | Browse | • 142.5.140.216 |
| | Kredi Karti Hesap #U00d6zeti - 4508xxxxxxxx0017.exe | Get hash | malicious | Browse | • 192.185.163.68 |
| | lod2.xlsx | Get hash | malicious | Browse | • 162.241.226.37 |
| | Contract and PO No.908876.exe | Get hash | malicious | Browse | • 192.185.84.191 |
| | iwah6jVhmw | Get hash | malicious | Browse | • 98.130.22.83 |
| | BL-210915L0.exe | Get hash | malicious | Browse | • 192.254.180.165 |
| | mFKC2tSCJX | Get hash | malicious | Browse | • 76.163.226.11 |
| | Urgent Inquiry.exe | Get hash | malicious | Browse | • 192.185.84.191 |
| | PO 007661721.exe | Get hash | malicious | Browse | • 192.185.84.191 |
| | P.I 099880990.xlsx | Get hash | malicious | Browse | • 162.214.65.211 |
| | 1QbmrgleyAWkb39.exe | Get hash | malicious | Browse | • 192.185.84.191 |
| | (RG25LGSJ).exe | Get hash | malicious | Browse | • 162.241.216.179 |
| | 103 Ref 2853801324189923.exe | Get hash | malicious | Browse | • 67.20.76.184 |
| | doc_0862413890.exe | Get hash | malicious | Browse | • 74.220.199.6 |
| | swift.Telex.xls | Get hash | malicious | Browse | • 192.185.115.3 |
| | g4225Fz3HK | Get hash | malicious | Browse | • 162.214.19.189 |
| | HBL-21706385 INV_2.exe | Get hash | malicious | Browse | • 192.254.180.165 |

## JA3 Fingerprints

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 7dcce5b76c8b17472d024758970a406b | INV.ppt | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | Purchase Order .xlsx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | MV JOLLY EXPRESS.docx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | DHL_Delivery_Notification.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | FedEx AWB 884174658339.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | UPDATE INVOICE FM K & S INDUSTRY.docx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | PO 347391.docx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | swift.Telex.xls | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | Invoice number 1257MAJAKFVII2021 incl. VAT.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | Consignment Notification.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | RFQ87976VF.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | RFQPTD0075453423.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | F#U0130YAT TEKL#U0130F#U0130 FORMU.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | CONTRACT 0902021.doc | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | PO006237_2nd Shipment.docx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | sample.exe | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | avec.xlsx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | SecuriteInfo.com.Trojan.GenericKD.37622653.5338.xlsm | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | SecuriteInfo.com.Trojan.GenericKD.37622653.5338.xlsm | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |
| | PO no 275.xlsx | Get hash | malicious | Browse | • 101.0.112.4<br>• 108.179.242.179<br>• 172.93.99.178 |

## 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: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Oct 12 08:22:59 2021, Security: 0 |
| Entropy (8bit): | 7.531872402672375 |
| TrID: | • Microsoft Excel sheet (30009/1) 78.94%<br>• Generic OLE2 / Multistream Compound File (8008/1) 21.06% |
| File name: | doc-220808714.xls |
| File size: | 241152 |
| MD5: | 2654fdca7197f542cbd0be823a2a2a9f |
| SHA1: | 149b43a5f8f4d9bd63720b408f6c4e2a86401c6a |
| SHA256: | f5a313c5353ae0d1cede7bd5e234bfd3a4d7abb5e877bd2903d8d7572e9ee4d6 |
| SHA512: | 1534994b08b95c1a9879afba6a857817146b3aaa06484a65ff89f418b5ca31fa7ffbc2076efdface8f0036f5e3a7f98e95fe0120df3bfe2c2b06ea8e3b96bcaf |
| SSDEEP: | 6144:cKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgq9jWXcZZRBTq1BOzTwvOsPDslAvS32vl7p:09jVzTmszTwvTDy33LvfP1OWr |
| File Content Preview: | .....>.....<br>.....<br>..... |

## File Icon

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

## Static OLE Info

### General

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

### OLE File "doc-220808714.xls"

#### Indicators

| | |
|---|---|
| Has Summary Info: | True |
| Application Name: | Microsoft 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: | 1251 |
| Author: | |
| Last Saved By: | |
| Create Time: | 2015-06-05 18:19:34 |
| Last Saved Time: | 2021-10-12 07:22:59 |
| Creating Application: | Microsoft Excel |

| Summary | |
|---|---|
| Security: | 0 |

| Document Summary | |
|---|---|
| Document Code Page: | 1251 |
| Thumbnail Scaling Desired: | False |
| Company: | |
| Contains Dirty Links: | False |
| Shared Document: | False |
| Changed Hyperlinks: | False |
| Application Version: | 1048576 |

**Streams**

# Network Behavior

## Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Oct 12, 2021 17:13:39.986201048 CEST | 192.168.2.22 | 8.8.8.8 | 0xe415 | Standard query (0) | ohemaa.org | A (IP address) | IN (0x0001) |
| Oct 12, 2021 17:13:41.872337103 CEST | 192.168.2.22 | 8.8.8.8 | 0xd9e3 | Standard query (0) | madieandme.com.au | A (IP address) | IN (0x0001) |
| Oct 12, 2021 17:13:45.575872898 CEST | 192.168.2.22 | 8.8.8.8 | 0x4c3b | Standard query (0) | amerident.com.do | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Oct 12, 2021 17:13:40.005583048 CEST | 8.8.8.8 | 192.168.2.22 | 0xe415 | No error (0) | ohemaa.org | | 172.93.99.178 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 17:13:42.188901901 CEST | 8.8.8.8 | 192.168.2.22 | 0xd9e3 | No error (0) | madieandme.com.au | | 101.0.112.4 | A (IP address) | IN (0x0001) |
| Oct 12, 2021 17:13:45.717439890 CEST | 8.8.8.8 | 192.168.2.22 | 0x4c3b | No error (0) | amerident.com.do | | 108.179.242.179 | A (IP address) | IN (0x0001) |

### HTTP Request Dependency Graph

- ohemaa.org
- madieandme.com.au
- amerident.com.do

### HTTPS Proxied Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.22 | 49165 | 172.93.99.178 | 443 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-10-12 15:13:40 UTC | 0 | OUT | GET /HUVm9mDKLW9C/ocrafhh.html HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: ohemaa.org<br>Connection: Keep-Alive |
| 2021-10-12 15:13:41 UTC | 0 | IN | HTTP/1.1 200 OK<br>Connection: close<br>x-powered-by: PHP/5.6.40<br>content-type: text/html; charset=UTF-8<br>content-length: 0<br>date: Tue, 12 Oct 2021 15:13:41 GMT<br>server: LiteSpeed<br>alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.22 | 49166 | 101.0.112.4 | 443 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-10-12 15:13:42 UTC | 0 | OUT | GET /xnkpOLnvlN6T/ocrafh.html HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: madieandme.com.au<br>Connection: Keep-Alive |
| 2021-10-12 15:13:45 UTC | 1 | IN | HTTP/1.1 200 OK<br>Connection: close<br>x-powered-by: PHP/7.2.34<br>content-type: text/html; charset=UTF-8<br>content-length: 0<br>date: Tue, 12 Oct 2021 15:13:45 GMT<br>server: LiteSpeed<br>vary: User-Agent<br>alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.22 | 49167 | 108.179.242.179 | 443 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| 2021-10-12 15:13:46 UTC | 1 | OUT | GET /xdOMlaB0XJ7/ocraf.html HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: ameridentcom.do<br>Connection: Keep-Alive |
| 2021-10-12 15:13:46 UTC | 1 | IN | HTTP/1.1 200 OK<br>Date: Tue, 12 Oct 2021 15:13:46 GMT<br>Server: nginx/1.19.10<br>Content-Type: text/html; charset=UTF-8<br>Content-Length: 0<br>X-Server-Cache: true<br>X-Proxy-Cache: HIT<br>Connection: close |

## Code Manipulations

## Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: EXCEL.EXE PID: 508 Parent PID: 596

### General

| | |
|---|---|
| Start time: | 17:13:20 |
| Start date: | 12/10/2021 |
| 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: | 0x13fa70000 |
| File size: | 28253536 bytes |
| MD5 hash: | D53B85E21886D2AF9815C377537BCAC3 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Moved

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: regsvr32.exe PID: 1212 Parent PID: 508

### General

| | |
|---|---|
| Start time: | 17:13:29 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test |
| Imagebase: | 0xff1e0000 |
| 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: 1444 Parent PID: 508

### General

| | |
|---|---|
| Start time: | 17:13:29 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test |
| Imagebase: | 0xff1e0000 |
| 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: 2792 Parent PID: 508

### General

| | |
|---|---|
| Start time: | 17:13:29 |
| Start date: | 12/10/2021 |
| Path: | C:\Windows\System32\regsvr32.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test |
| Imagebase: | 0xff1e0000 |
| 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