
**ID:** 435316
**Sample Name:** PO-0814.doc
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 12:07:17
**Date:** 16/06/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents

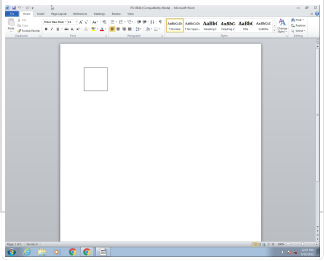
# Windows Analysis Report PO-0814.doc

## Overview

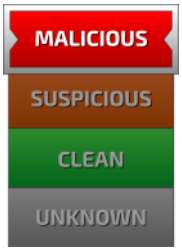
### General Information

| | |
|---|---|
| Sample Name: | PO-0814.doc |
| Analysis ID: | 435316 |
| MD5: | c811bfeba8f5ecd.. |
| SHA1: | 32bd41b37872d0.. |
| SHA256: | fe5b31f0bf9c8a1… |
| Tags: | doc |
| Infos: | |

Most interesting Screenshot:



### Detection

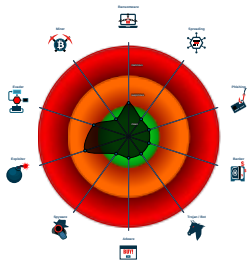



| | |
|---|---|
| Score: | 56 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Internet Provider seen in connection…
- May sleep (evasive loops) to hinder …
- Office Equation Editor has been star…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

### Classification



## Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2496 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1320 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- EQNEDT32.EXE (PID: 2868 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **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:

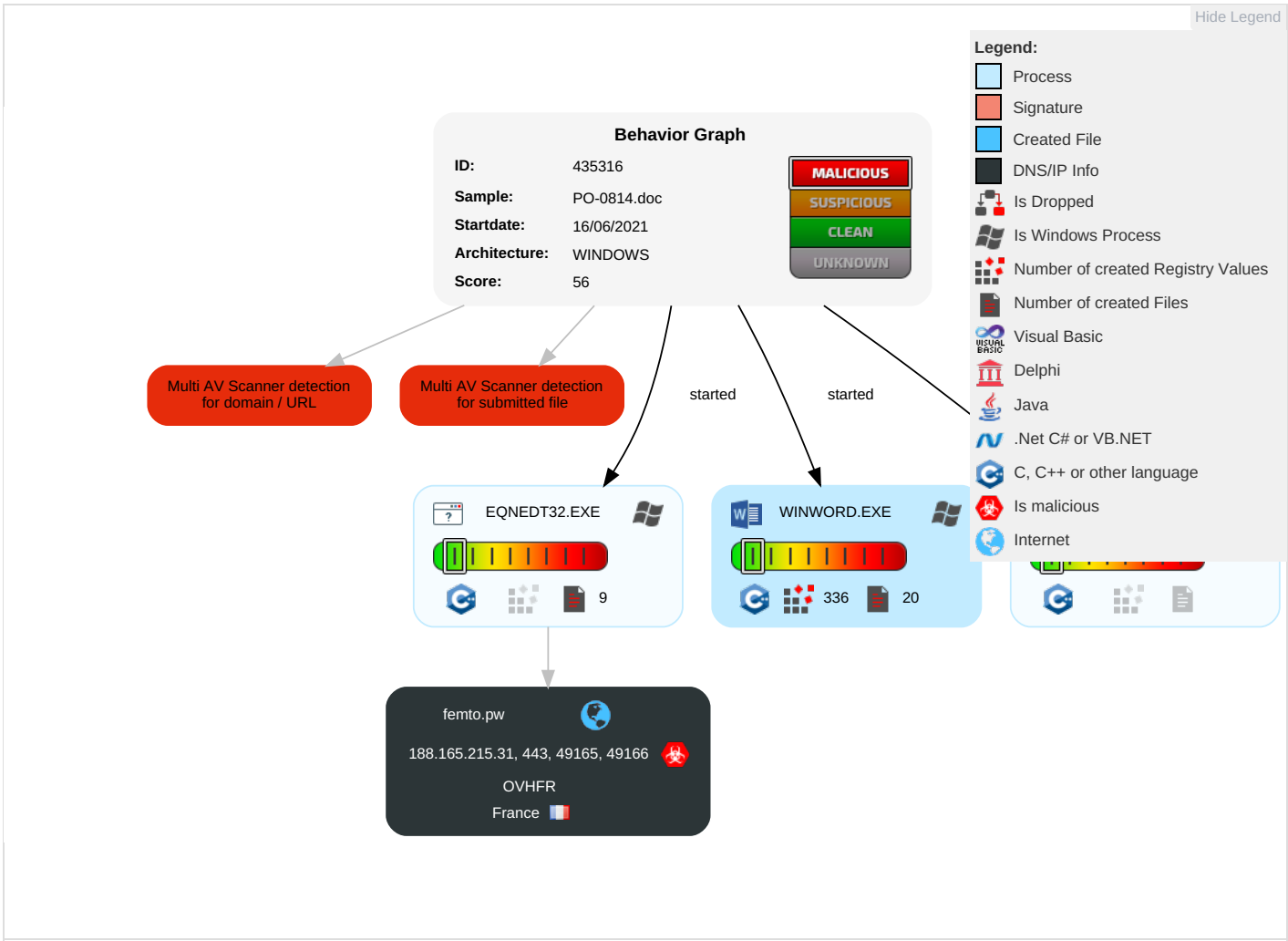
**Multi AV Scanner detection for domain / URL**

**Multi AV Scanner detection for submitted file**

## 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Exploitation for Client Execution 3 | Path Interception | Process Injection 1 | Masquerading 1 | OS Credential Dumping | Virtualization/Sandbox Evasion 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 2 | Eavesdrop on Insecure Network Communication | Remotel Track D Without Authoriz |
| Default Accounts | Scheduled Task/Job | 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 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotel Wipe Da Without Authoriz |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Process Injection 1 | Security Account Manager | System Information Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 2 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Binary Padding | NTDS | Remote System Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Ingress Tool Transfer 1 | SIM Card Swap | |

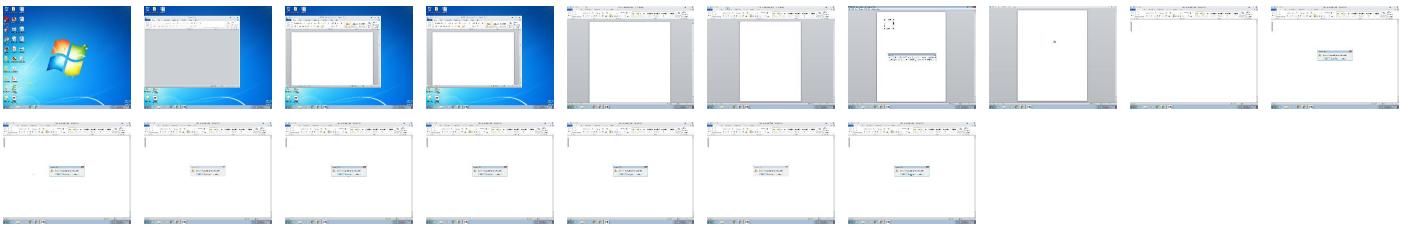
## Behavior Graph

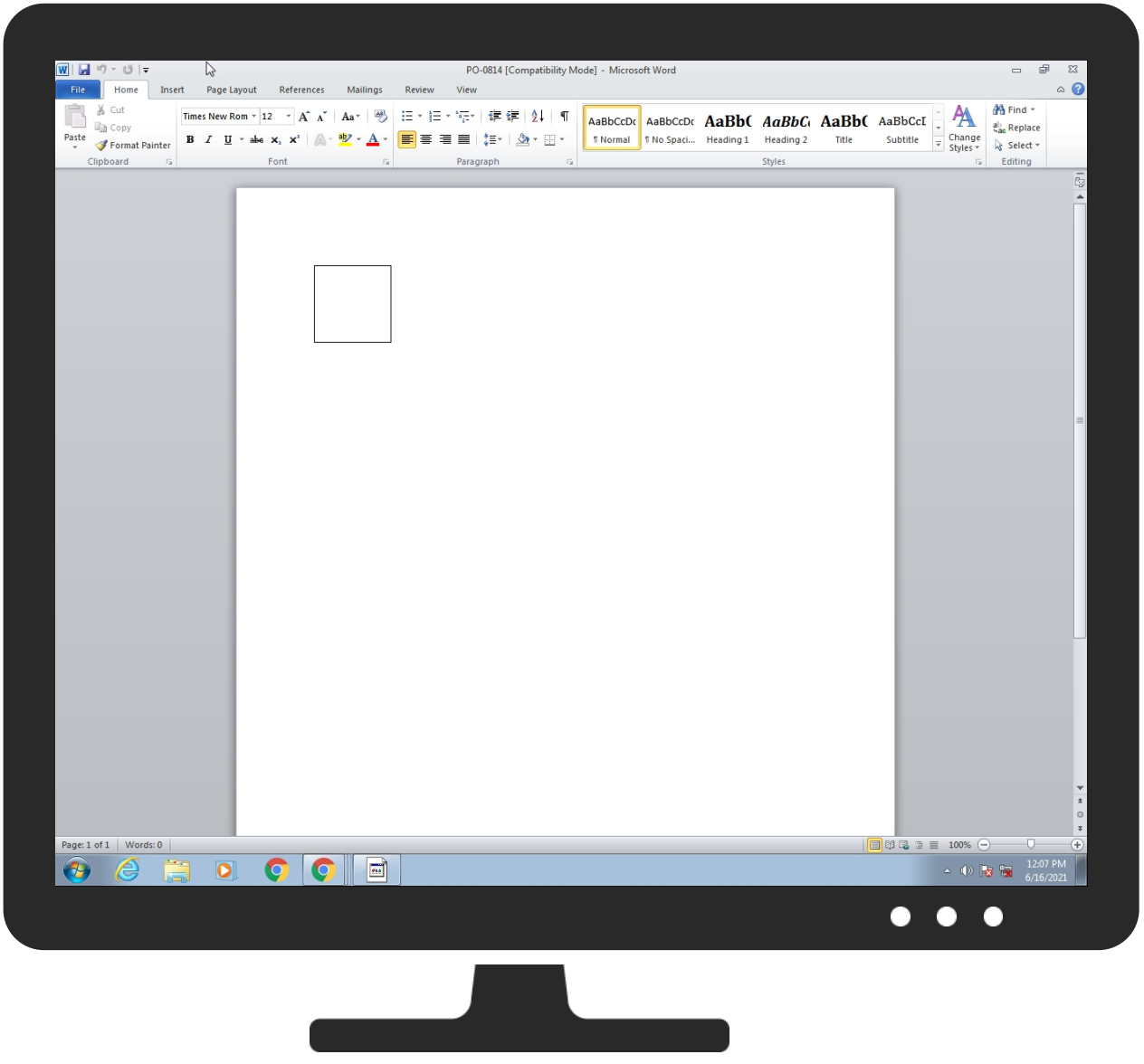


# Screenshots

## 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 |
|---|---|---|---|---|
| PO-0814.doc | 35% | ReversingLabs | Document-Office.Exploit.CVE-2017-11882 | |

## Dropped Files

**No Antivirus matches**

## Unpacked PE Files

No Antivirus matches

## Domains

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| femto.pw | 6% | Virustotal | | Browse |

## URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

| Name | IP | Active | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|---|---|
| femto.pw | 188.165.215.31 | true | true | • 6%, Virustotal, Browse | unknown |

## Contacted IPs

## Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 188.165.215.31 | femto.pw | France | | 16276 | OVHFR | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |
| Analysis ID: | 435316 |
| Start date: | 16.06.2021 |
| Start time: | 12:07:17 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 4m 18s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | PO-0814.doc |
| 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: | 7 |
| 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: | mal56.winDOC@3/6@2/1 |

| | |
|---|---|
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .doc<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Active ActiveX Object<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 12:07:34 | API Interceptor | 241x Sleep call for process: EQNEDT32.EXE modified |

# Joe Sandbox View / Context

## IPs

**No context**

## Domains

**No context**

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| OVHFR | jqJ9rVHXq0LCZ6R.exe | Get hash | malicious | Browse | • 54.36.120.230 |
| | SecuriteInfo.com.BackDoor.Rat.281.18292.exe | Get hash | malicious | Browse | • 198.245.49.191 |
| | RFQ Products.xlsx | Get hash | malicious | Browse | • 167.114.158.9 |
| | DocumentCopy_pdf.exe | Get hash | malicious | Browse | • 213.186.33.5 |
| | Proforma Invoice & Bank Swift Copy.exe | Get hash | malicious | Browse | • 51.79.149.34 |
| | Profoma Invoice1506021.exe | Get hash | malicious | Browse | • 158.69.138.23 |
| | kkaH2ZEdQ1.exe | Get hash | malicious | Browse | • 213.186.33.5 |
| | LDOsa1uqyb.exe | Get hash | malicious | Browse | • 176.31.56.216 |
| | Quotation.exe | Get hash | malicious | Browse | • 192.99.208.14 |
| | LSMD.exe | Get hash | malicious | Browse | • 37.187.95.110 |
| | IHdviiaZ7h.exe | Get hash | malicious | Browse | • 51.195.61.169 |
| | 7#U1d05.html | Get hash | malicious | Browse | • 51.89.21.20 |
| | 03soKqWLfN.exe | Get hash | malicious | Browse | • 51.89.96.41 |
| | bpkuoAqilk.exe | Get hash | malicious | Browse | • 176.31.95.228 |
| | Wire_receipt.exe | Get hash | malicious | Browse | • 5.135.115.129 |
| | Shipping Doc578.exe | Get hash | malicious | Browse | • 213.186.33.5 |
| | URGENT REQUEST FOR QUOTATION (RFQ REF R 2100131410).exe | Get hash | malicious | Browse | • 51.91.236.193 |
| | Reference No. # 3200025006.exe | Get hash | malicious | Browse | • 213.186.33.5 |
| | Cancellation_Letter_2137859823_06112021.xlsm | Get hash | malicious | Browse | • 51.254.164.254 |
| | Cancellation_Letter_2137859823_06112021.xlsm | Get hash | malicious | Browse | • 51.254.164.254 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1BF24CA3-025D-4403-9DBE-B492A11253DC}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1024 |
| Entropy (8bit): | 0.05390218305374581 |
| Encrypted: | false |
| SSDEEP: | 3:ol3lYdn:4Wn |
| MD5: | 5D4D94EE7E06BBB0AF9584119797B23A |
| SHA1: | DBB111419C704F116EFA8E72471DD83E86E49677 |
| SHA-256: | 4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1 |
| SHA-512: | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | ..... ..... ..... ..... |

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3A3DB071-4F03-4D2B-8C5C-F1ADB9722678}.tmp | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1024 |
| Entropy (8bit): | 0.8014421130618178 |
| Encrypted: | false |
| SSDEEP: | 3:gl2lfgREqAWlglqlg7tlNl7lY2l/Dlll8v0lglwZlDZt3UlglwZel8gl7vII8:zNgREqAWlgFJMSDlll8vlwLf3FwQFrB |
| MD5: | EB0751D3AFEABB0642BCE1B447B56873 |
| SHA1: | 185B5B1DE228A51B29E026673C6A09B5B02D4B3A |
| SHA-256: | 053868F5B2500C65687C650D6A028B267ADA27D44BF0243D8A61A42147002FF5 |
| SHA-512: | BC423BD78BBC6E4DD3B284C25616D8952E8285B7719A470175A2356AFEA0837B0079602A9FC0513044ACCD6051A01A3C3A86F020D38EFC1D149855C4015577BF |
| Malicious: | false |
| Reputation: | low |
| Preview: | =..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ..... ..... .....j....CJ..OJ..QJ..U..^J..aJ.. .j.htd...CJ..OJ..QJ..U..^J..aJ. |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO-0814.LNK | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:14 2020, mtime=Wed Aug 26 14:08:14 2020, atime=Wed Jun 16 18:07:31 2021, length=1710047, window=hide |
| Category: | dropped |
| Size (bytes): | 1994 |
| Entropy (8bit): | 4.5282245969604675 |
| Encrypted: | false |
| SSDEEP: | 48:8O/XT0jFTH4ysHWsQhQh2O/XT0jFTH4ysHWsQhQ/:8O/XojFzTs2sQhQh2O/XojFzTs2sQhQ/ |
| MD5: | A62E239B31671BD354E7092F5AD93AD0 |
| SHA1: | E59BDFF4F89D80CD8ED4DCC5091B6BF5890FCF8C |
| SHA-256: | 6D237667C00BCAE14F95BCDF278F6A75B0B241F35B5B0B45A1847479F6E2CFE0 |
| SHA-512: | 8CD51EDBC6D79611F5E2718D96CEBC5248630C9126771C132841E19ACAEB7C8E9337E73947C34A2ECD90E167BC02DD05829D9343B5BA9325836FB6332970E9F |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.....F.... .....{.....{..x)...b.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....^.2.....R. .PO-0814.doc.D.....Q.y.Q.y*...8.....P.O.-.0.8.1.4...d.o.c.....u.....-...8...[.....?J.....C:\Users\..#.....\\651689\Users.user\Desktop\PO-0814.doc."....\....\....\....\....\.D.e.s.k.t.o.p.\.P.O.-.0.8.1.4...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....651689.....D_....3N...W...9F.C.....[D_....3N...W...9F.C.....[....L.. |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | ASCII text, with CRLF line terminators |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
|---|---|
| Category: | dropped |
| Size (bytes): | 59 |
| Entropy (8bit): | 4.1702223972093195 |
| Encrypted: | false |
| SSDEEP: | 3:M1gAOru4otDOru4omX1gAOru4ov:MiAO5mDO5IAO5y |
| MD5: | 7658D96DC6F1BF1C4B8E7587B63785BF |
| SHA1: | 9EA85D1D15BEC75AB16A6F14A8074B15006E4821 |
| SHA-256: | 96787D74AC1F603009D6AF517C2100C4FF79E947097BE74A818B876FEA1FE61D |
| SHA-512: | 195D14A0ED4D61CA6ABDA1302FC75A684E57B760486EAB5D7B60D0A2B3F1B0AA2BDFE2DDCF2726A1B9118B4B322322E919E922C34E702888C307E3D82A4677<br>6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | [doc]..PO-0814.LNK=0..PO-0814.LNK=0..[doc]..PO-0814.LNK=0.. |

| C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.4070851566761475 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVy/KbSjgzGwzFF24ilH/ln:vdsCkWtZbXPFridl |
| MD5: | 40DB84241CC0B8BC853E1806AADC46A5 |
| SHA1: | CFC905CEB89AC86F6CC7D21FB5F0359AFF5A8464 |
| SHA-256: | 9973DA893D7F11A27803AC08DCE92F17793C8DC96FB51A6B1174BDD367976FA5 |
| SHA-512: | 77D71BC60A3C6FBE38D56DE49DC139C2F10644584399AAFC49C429359EB5FD301BC6E02A43456F838826A30D2A6EAB0D4D0B4D5761C60D3410A5FD1CC0C5E0<br>4 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .user.....A.l.b.u.s.....p.....P.....z.....x... |

| C:\Users\user\Desktop\~$O-0814.doc | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.4070851566761475 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVy/KbSjgzGwzFF24ilH/ln:vdsCkWtZbXPFridl |
| MD5: | 40DB84241CC0B8BC853E1806AADC46A5 |
| SHA1: | CFC905CEB89AC86F6CC7D21FB5F0359AFF5A8464 |
| SHA-256: | 9973DA893D7F11A27803AC08DCE92F17793C8DC96FB51A6B1174BDD367976FA5 |
| SHA-512: | 77D71BC60A3C6FBE38D56DE49DC139C2F10644584399AAFC49C429359EB5FD301BC6E02A43456F838826A30D2A6EAB0D4D0B4D5761C60D3410A5FD1CC0C5E0<br>4 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .user.....A.l.b.u.s.....p.....P.....z.....x... |

# Static File Info

## General

| | |
|---|---|
| File type: | Rich Text Format data, unknown version |
| Entropy (8bit): | 3.5422390551490244 |
| TrID: | • Rich Text Format (5005/1) 55.56%<br>• Rich Text Format (4004/1) 44.44% |
| File name: | PO-0814.doc |
| File size: | 1710047 |
| MD5: | c811bfeba8f5ecd3fa4fe6e65dcc46af |
| SHA1: | 32bd41b37872d0bd3d6376abbb29b8d0da47f1ac |
| SHA256: | fe5b31f0bf9c8a120cd21da9a474ca1b083af0e23ee0e29<br>ca42939009aa4e149 |

### General

| | |
|---|---|
| SHA512: | 9b79c8edee042ed6746c9c9e7a6693c9bced573c11c055<br>0aaddea0459b480e6e97a3900e132687b33604e91ba9ef<br>af99df4fc3406092578f67d6d48b021946f0 |
| SSDEEP: | 12288:2NpPfQ5Q48Fr8jzOpbXW84abtMCF2XdO/hTtGL<br>6oRkrG2X4:2NpPfQe4ZmpbGs32XdO3GL7+G2X4 |
| File Content Preview: | {\rtf6965{\object\objautlink70169935\objw9723\objh6132<br>{*\objdata.9c9bd81a020000000b000004571756174496<br>f4e2e330000000000000000009d0b0d00037e01eb470a0<br>105d76448ec0000000000000000000000000000000000<br>000000000000005006450000000000000000000000000<br>00000000000000 |

### File Icon

| | |
|---|---|
| Icon Hash: | e4eea2aaa4b4b4a4 |

### Static RTF Info

#### Objects

| Id | Start | Format ID | Format | Classname | Datasize | Filename | Sourcepath | Temppath | Exploit |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0000003Dh | 2 | embedded | EquatIoN.3 | 854941 | | | | no |

## Network Behavior

### Network Port Distribution

### TCP Packets

### UDP Packets

### DNS Queries

| Timestamp | Source IP | Dest IP | Trans ID | OP Code | Name | Type | Class |
|---|---|---|---|---|---|---|---|
| Jun 16, 2021 12:08:08.262192965 CEST | 192.168.2.22 | 8.8.8.8 | 0xfc39 | Standard query (0) | femto.pw | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:08:08.324449062 CEST | 192.168.2.22 | 8.8.8.8 | 0xfc39 | Standard query (0) | femto.pw | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp | Source IP | Dest IP | Trans ID | Reply Code | Name | CName | Address | Type | Class |
|---|---|---|---|---|---|---|---|---|---|
| Jun 16, 2021 12:08:08.324176073 CEST | 8.8.8.8 | 192.168.2.22 | 0xfc39 | No error (0) | femto.pw | | 188.165.215.31 | A (IP address) | IN (0x0001) |
| Jun 16, 2021 12:08:08.386293888 CEST | 8.8.8.8 | 192.168.2.22 | 0xfc39 | No error (0) | femto.pw | | 188.165.215.31 | A (IP address) | IN (0x0001) |

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

# System Behavior

## Analysis Process: WINWORD.EXE PID: 2496 Parent PID: 584

### General

| | |
|---|---|
| Start time: | 12:07:32 |
| Start date: | 16/06/2021 |
| Path: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding |
| Imagebase: | 0x13f1e0000 |
| File size: | 1424032 bytes |
| MD5 hash: | 95C38D04597050285A18F66039EDB456 |
| 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: EQNEDT32.EXE PID: 1320 Parent PID: 584

### General

| | |
|---|---|
| Start time: | 12:07:33 |
| Start date: | 16/06/2021 |
| Path: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding |
| Imagebase: | 0x400000 |
| File size: | 543304 bytes |
| MD5 hash: | A87236E214F6D42A65F5DEDAC816AEC8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

### Registry Activities

Show Windows behavior

**Key Created**

## Analysis Process: EQNEDT32.EXE PID: 2868 Parent PID: 584

### General

| | |
|---|---|
| Start time: | 12:07:52 |
| Start date: | 16/06/2021 |
| Path: | C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding |
| Imagebase: | 0x400000 |
| File size: | 543304 bytes |
| MD5 hash: | A87236E214F6D42A65F5DEDAC816AEC8 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

### Registry Activities

Show Windows behavior

# Disassembly