Lab 03: Excel 4

**Required Environment:** Remnux 7 V VM, Windows 7/10 VM

**Required Software:**

On Remnux, you need Xlmdeobfuscator, Oledump, Olevba3, Msoffoffcrypto-tool

On Windows 7, you need Excel, Oledump, hXd

* Complete this work using the tools provided. Do not use open source reference material or sandboxes. Use only the indicated tools.

**Goal:** The goal of this lab is to gain familiarity with Excel 4 and some tools and techniques to help deal with Excel 4 macros.

**Useful Commands:**

**Msoffcrypto-tool** can help determine if an Excel document has been encrypted.

Check to see if it is encrypted:

* msoffcrypto-tool --test -v enc.xls

If an Excel document has been encrypted, this can be used to help decrypt it.

* msoffcrypto-tool -p VelvetSweatshop file.xls file-decrypted.xls

**Oledump** can help extract streams and also utilize the plugin\_biff plugin for Excel 4 macros.

Extract a stream:

* oledump file.xls -s 23 -v

Extract XLM content:

* oledump file.xls -p plugin\_diff

Check to see if very hidden sheets:

* oledump file.xls -p plugin\_diff –pluginoptions “-x”

Check to see the hex for very hidden sheets:

* oledump file.xls -p plugin\_diff –pluginoptions “-o BOUNDSHEET -a”
  + Note: this seems to work only on Windows

**xlmdeobfuscator** can help pull apart Excel 4 macros

* xlmdeobfuscator -f interestingFile.xls

**Useful links:**

* Maldocs Cheatsheet
  + <https://fareedfauzi.github.io/notes/Maldoc-notes-cheatsheet/#>
* Excel 4 References PDF
  + <https://d13ot9o61jdzpp.cloudfront.net/files/Excel%204.0%20Macro%20Functions%20Reference.pdf>

**Task 1 - 213f3ec5d3fdd5ae0e0ab3744f8147dc**

* This malware is password protected; its password is **1234.** Use msoffcrypto-tool to decrypt it. This one has countless hidden sheets, but xlmdeobfuscator will allow you to deobfuscated these, so it is not necessary to unhide these.
* What directories does it create?
* How does it make use of different API’s to achieve its objective of downloading the next stage—which API’s does it use and what is it using them to do?

**Task 2 - d0313772c1e64397f258f4d2858b6887.bin drops Qakbot**

* What files are being downloaded?
* How do you approach this malware—what tools did you use to deobfuscate it?
* What is the method it uses to get the payload to execute and reach the second stage—describe it.
* What is being registered?

**Task 3 - 488543905f161a9a35434299ad6474c6.bin**

* Where is the file being downloaded from this?
* How complex is this malware?
* How many hidden sheets are there? Does unhiding it seem to add anything new?

**Task 4 - 82c12e7fe6cabf5edc0bdaa760b4b8c8.bin**

* What are some of the anti-analysis checks used in this malware? Why do you think these ones have been chosen?
* What are some of the anti-analysis checks in place here?
* What is likely the final payload executed?