Principles of Using Debuggers in Document Analysis

Learning Objectives

- Why debuggers work
- What to monitor
- Debugging Tools

Programs and Scripts

```
Dim fso as Object
Set fso = CreateObject("Scripting.FileSystemObject")
Dim oFile as Object
Set oFile = FSO.CreateTextFile("bad.ps1")
oFile.WriteLine "malware code"
oFile.Close
```

```
hFile = CreateFileW("bad.ps1", …)
WriteFile(hFile, "malware code", …)
CloseFile(hFile)
```

Functions to Monitor

File Operations	HTTP Operations	Process Operations
CreateFileW	InternetCrackURL	CreateProcess
WriteFile	HTTPCrackURL	

Debuggers

```
Dim fso as Object
Set fso = CreateObject("Scripting.FileSystemObject")
Dim oFile as Object
Set oFile = FSO.CreateTextFile("bad.ps1")
oFile.WriteLine "malware code"
oFile.Close
```

```
hFile = CreateFileW("bad.ps1", …)
WriteFile(hFile, "malware code", …)
CloseFile(hFile)
```

Lazy Office Analyzer

Extracts URLs, file modifications, and executed programs

Word, Excel, PowerPoint, and JavaScript

https://github.com/tehsyntx/loffice

Options

Loffice.py type exit-on FILENAME

Type: word, excel, power, script

Exit-on: url, proc, none

Lazy Office Analyzer Prerequistes

- Microsoft Office
- WinDbg - https://msdn.microsoft.com/en-us/windows/hardware/hh852365
- Python 2.7
- WinAppDbg - http://winappdbg.sourceforge.net/

Use pip to install:

- pefile - https://github.com/erocarrera/pefile
- capstone - https://pypi.python.org/pypi/capstone-windows

Thank you