A-3-1
標的型攻撃メールと添付ファイルのマルウェア(静的)解析

中部大学
岡部　仁

目的

A教授に送られた植木総務課長からのメール調査
・メールヘッダの解析
・添付ファイルの解析

① メールヘッダを解析し、メール送信先および問題点を把握する方法を理解する。
② 添付ファイルの概要解析方法(正常なファイルでない)を理解する。

メニュー

1. メールヘッダの解析： 演習3-1
2. 標的型メール調査の着目点
   - メールヘッダ
   - 本文表記
3. 添付ファイルの解析: 演習3-2, 3-3
   ① ファイル種別の調査
   ② 不正な添付ファイル情報の確認
   - ツール
   - オンラインWebサイトの利用
4. まとめ

標的型メール調査の着目点

- メールヘッダ情報
  - 送信経路が不審: 何処のメールサーバ経由したのか？
  - 文字コードが不審：「?GB2312?B?」中国語（簡体）？
  - 送信日時、タイムゾーン（GMT+?)が不審： +0800
  - メーラーが不審： 知らないもの？
- メーラーソフトの送信簿、メールサーバのログ
- 本文表記
  - 書き出し挨拶、括り表記の違い
  - URL
  - 添付ファイル（圧縮形式： rar形式（東欧、共産国）
- その他

添付ファイルの解析

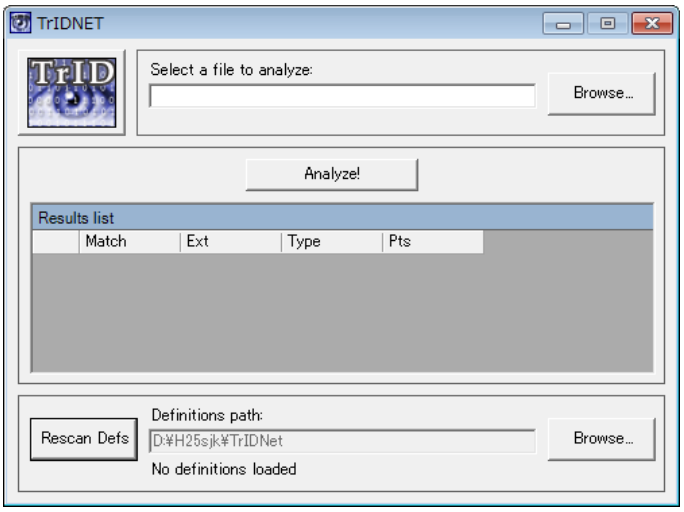
- 添付ファイルへのマルウェア(Dropper)の混入
  - 特段、ファイル実行時に異常動作(表記)はない
  - しばらく、何もしないものもある(Sleep)
- ファイル修飾子が必ずしも正しくない： ファイル種別調査(議事録.docは?)
- ファイル種別によって解析ツールが異なる(例)
  - Microsoft Office, 一太郎文書ファイル： OfficeMalScanner
  - RTFファイル： OfficeMalScanner(RTFScan.exe)
  - PDFファイル： PDF Stream Dumper
  - Flashファイル： SWFRETools, Adobe SWF Investigator
  - 実行ファイル： Yara

ファイル種別

- Windows上で動作するマルウェア種類
  - PE(Portable Executable)形式の実行可能なファイル
    - 実行ファイル： exe
    - ダイナミックリンクライブラリ： dll
    - スクリーンセーバ： scr
    - ActiveXコントローラ： ocx
    - ドライバーファイル，キーロガー(ルートキット)： sys
  - 文書ファイル(OLE2：
    - Microsoft Office, 一太郎ファイル： doc, xlsなど
    - Rich Textファイル： rft
    - PDFファイル： pdf
  - スクリプト： VBScript, Python, Rubyなどのインタプリタ
  - Adobe Flashファイル： swf

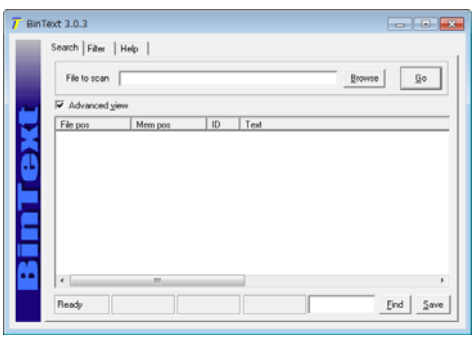
ファイル種別の判定

- 添付ファイル： 議事録.doc
- ツール：TrIDNet（演習3-1）



ファイルの表層解析（サーフィス解析）

- マルウェアに含まれる文字列の抽出
  - 通信先のIPアドレスやドメイン名
  - アクセスするパス名ファイル名
  - アクセスレジストリ
  - アクセスするプロセス名やウィンドウ名
  - 使用するWin32API名
  - 実行するShellコマンド
- ツール： BinText(演習3-2）

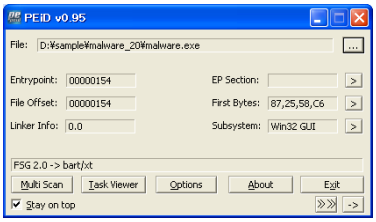


シェルコート,Exploitコードの暗号処理

- BinTextでは有効情報が得られない
- XORにより暗号処理

  OfficeMalScanner malware.xls scan **brute**
- PEファイルのパッカー

  感染活動に必要な文字列がすべて圧縮され、可読性のないものに専用ツールで変換
  - アンパッカー判定ツール： PEiD
  - 可読化し、BinText

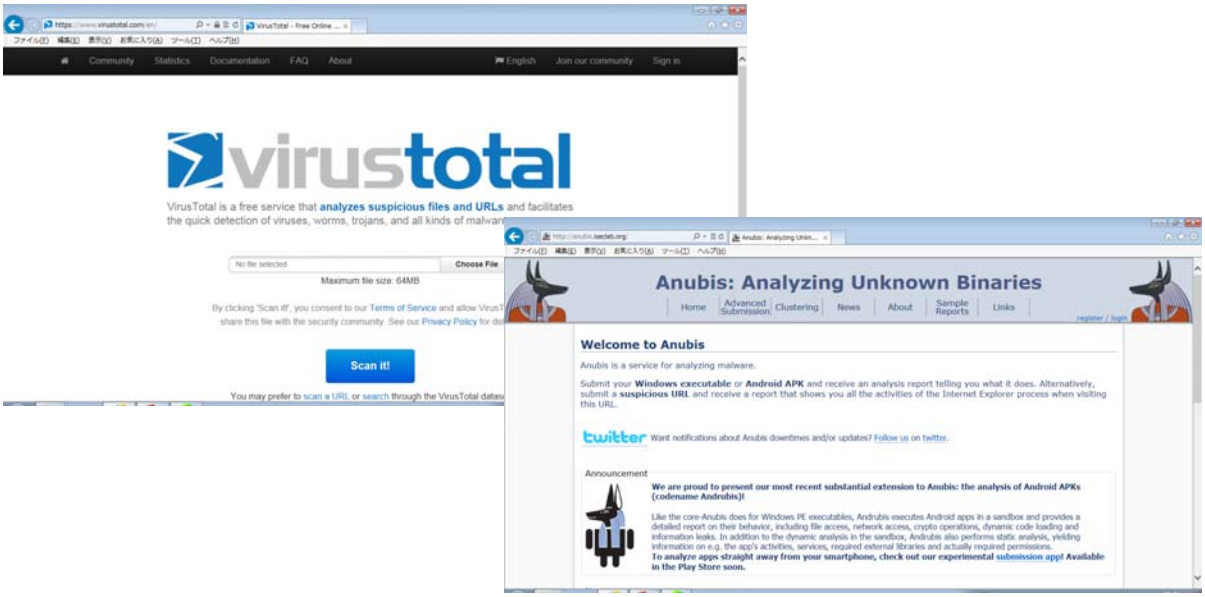


添付ファイル解析

- OfficeMalScanner（演習3-3)
  - RTFScan.exe
  - OfficeMalScanner.exe
- 添付ファイルのマルウェアの有無
- 詳細解析は、専門メーカーに依頼、その判断に

動的解析Webサービス

- VirusTotal: http://www.virustotal.com/　デモ
- Anubis: http://anubis.iseclab.org/



議事録.docの実態

- ファイル名: Laden'sDeath.doc

  Rich Text Formatの脆弱性を悪用するコードCVE-2010-3333
- CVE: Common Vulnerabilities and Exposures(共通脆弱性識別子: 個別製品中の脆弱性に一意の識別番号)

まとめ

- 組織内から標的型メールの送信があった事実
  - 報告と事後対応判断情報の提供
  - 詳細解析は専門家（有料）
  - 感染経路が特定できれば望ましい
  - 継続的な出口（対策）管理: ハッキングツールの通信
- マルウェア付メールの処分
- その他のPCの感染調査と拡散防止
  - 総務課長のPC
  - 総務課（苦情係）のPC
  - その他
- タイムライン解析

参考資料

- 標的型攻撃　セキュリティガイド
  岩井博樹 著、ソフトバンククリエイティブ株式会社

- アナライジング・マルウェア
  新井悠 他著、株式会社オライリー・ジャパン