卒業論文に向けて(2)

学部4年生
島本 大輔
2004年10月29日

概要

- 題材選び
- 今後の予定

題材選び

- ウィルス対策
  - ウィルス from パッチ
  - Detours みたいなライブラリ
  - 未知のウィルスを検知

題材選び

- ウィルス対策
  - ウィルス from パッチ
  - Detours みたいなライブラリ
  - 未知のウィルスを検知

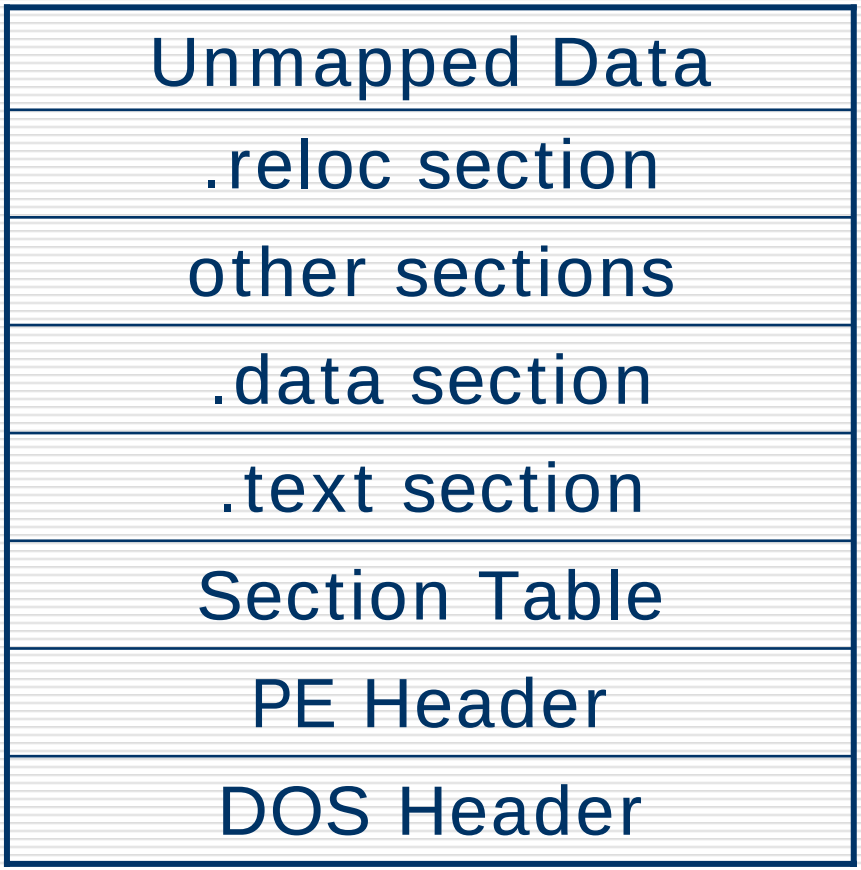
ウィルス from パッチ

- パッチを知る必要あり
  ＝ ファイル形式を知る必要あり
- 例：Windows では Portable Executable

Portable Executable

- Windows **の実行形式**
  - .exe, .dll, **など**
- **おおもとは** VAX/VMS **の** Common Object File Format (COFF)
- Portable **⇔ どのアーキテクチャ上でも**
  - Alpha, WindowsCE, **など**

Portable Executable Format



題材選び

- ウィルス対策
  - ウィルス from パッチ
  - Detours みたいなライブラリ
  - 未知のウィルスを検知

Detours

- Win32 API **のフックが可能**
- Microsoft Research
  http://www.research.microsoft.com/sn/detours/
- **ソースコードも公開されている**
  - **必死に解読中**

題材選び

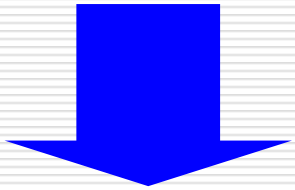
- ウィルス対策
  - ウィルス from パッチ
  - Detours みたいなライブラリ
  - 未知のウィルスを検知

未知のウィルスの発見

- プログラムを監視下で実行
  - つまりは、Sandbox
  - Win32 APIをフック＆引数をチェック
  - Linux におけるシステムコール監視の技術を応用（？）
- 現在、様々なウィルスやハッキング手法を調査中

APIのフック

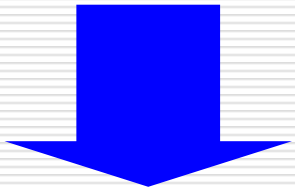
- Win32 APIのチェックが必要



- Detours のソースコードの理解
- Windows の仕組みの理解
  - PEファイルなど

Hacking & Virus on Windows

- **まずは敵を知ることから**



- **各種** exploit code **や** Virus code **を調査中**
  - Web**ページ上に“多く”あり**

参考文献(1)

- An In-Depth Look into the Win32 Portable Executable File Format (Part 1 & 2)
  - http://www.msdn.microsoft.com/msdnmag/issues/02/02/PE/default.aspx
  - http://www.msdn.microsoft.com/msdnmag/issues/02/03/PE2/default.aspx
- Process-wide API spying
  - http://www.codeproject.com/system/api_spying_hack.asp
- API Spying Techniques
  - http://www.internals.com/articles/apispy/apispy.htm

参考文献(2)

- detours
  - http://research.microsoft.com/sn/detours/
- Phrack
  - http://www.phrack.org/
- packet storm
  - http://www.packetstromsecurity.org/
- New order
  - http://neworder.box.sk/index.php
- VX heavens
  - http://vx.netlux.org/