龍谷大学理工学部における ウイルス感染事例

龍谷大学理工学部
小島　肇

背景となる状況

Story Backgrounds

龍谷大学

- 標準のアンチウイルスソフトとして、マカフィー製品を導入
- Windows:VirusScan Enterprise (VSE)
- Mac:VirusScan for Mac

The following take place between 2009.01 and 2009.02.

これは 2009.01 から 2009.02 に起こった出来事である

ウイルスに感染したらしいと連絡が入る

- 某研究室から：昨年ひどい目に会った人
- あまりにひどい目にあったため、この人はVirusScan Enterprise ではなくウイルスバスター 2009 を独自に購入して運用していた
- 使いまわしている USB メモリをウイルスバスターな機械に刺したら反応したので連絡
  - autorun もの
- 同じ USB メモリをVirusScan Enterprise な機械に刺しても無反応……

既にヤラレてた

その USB メモリはどこで使ったの？

- 共同利用している測定装置に刺した……

- もしかして、その測定装置を共同で使っている研究室は全滅ですか?!

研究室単位で

玉砕

していることを確認

生存者発見

- ウイルスバスター 2009 を使っていた
- Windows Vista を使っていた

一撃目はどこから？

- 今回の事例は学生の持ち込み PC か？
- アンチウイルスソフトは当然のように……

考察

Considerations

やめてほしい

- Windows XP
- 期限切れアンチウイルスソフト
- ノーガード戦法

使ってほしい

- Windows Vista / 7
- Microsoft Security Essentials
  http://www.microsoft.com/security_essentials/?mkt=ja-jp

やってほしい

- Microsoft Update
  - Office を更新していない人を多数発見
- アプリケーションのアップデート
  - Flash Player
  - Adobe Reader / Acrobat
  - QuickTime
  - Firefox
- 自動再生における自動実行の除外（Windows 7 と同じ挙動）
  - KB971029 更新プログラム
    http://support.microsoft.com/kb/971029/ja

やってほしい

- アンチウイルスソフトの更新状況の確認

その他

- 多様性は正義
- どのように駆除したかについては、http://www.st.ryukoku.ac.jp/blog/vuln/0114 を参照
- Artemis テクノロジーを実地に検証する機会はまだ得られていない

質問？