龍谷大学理工学部における ウイルス感染事例 part 2

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

龍谷大学
現在

Ryukoku University
Present Time

ウイルスとの闘いは続いていた

from “ALIENS”

周り中反応だらけだ！

from “ALIENS”

周り中反応だらけだ！ (proxy sever's log)

133.83.a.a - - [03/Dec/2009:19:14:27 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.a.a - - [03/Dec/2009:19:14:27 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327

133.83.a.c - - [03/Dec/2009:16:51:28 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.a.c - - [03/Dec/2009:16:51:28 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.a.c - - [03/Dec/2009:16:52:04 +0900] "GET http://www.googledf2.com/1rb/ar1.rar HTTP/1.0" 200 459
133.83.a.c - - [03/Dec/2009:16:52:06 +0900] "GET http://www.yahoo1xh.com/1rb/ar.rar HTTP/1.0" 401 1325
133.83.a.c - - [03/Dec/2009:16:52:06 +0900] "GET http://www.yahoo1xh.com/1rb/ar.rar HTTP/1.0" 401 1325
133.83.a.c - - [03/Dec/2009:16:52:27 +0900] "GET http://mk27w.com/1rb/ar1.rar HTTP/1.0" 200 401
133.83.a.c - - [03/Dec/2009:16:53:07 +0900] "GET http://www.googledf2.com/1rb/ar1.rar HTTP/1.0" 200 401
133.83.a.c - - [03/Dec/2009:16:56:29 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327

133.83.f.g - - [03/Dec/2009:13:08:36 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.f.g - - [03/Dec/2009:13:08:36 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.f.h - - [03/Dec/2009:12:17:25 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.f.h - - [03/Dec/2009:12:17:25 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.i.j - - [03/Dec/2009:19:57:29 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.i.j - - [03/Dec/2009:19:57:29 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1336
133.83.k.l - - [03/Dec/2009:10:39:51 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.k.l - - [03/Dec/2009:10:39:51 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.m.n - - [03/Dec/2009:16:28:31 +0900] "GET http://www.sinax7l.com/1rb/ar1.rar HTTP/1.0" 200 459
133.83.m.n - - [03/Dec/2009:16:28:32 +0900] "GET http://www.yahoo1xh.com/1rb/ar.rar HTTP/1.0" 401 1325
133.83.m.o - - [03/Dec/2009:16:28:18 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327
133.83.m.o - - [03/Dec/2009:16:28:18 +0900] "GET http://www.yahoo1xh.com/1rb/ar1.rar HTTP/1.0" 401 1327

最近のヤラレパターン

- ウイルス定義ファイルは正常に更新されているけれど、アンチウイルスソフトウェアは何の役にも立っていない

Artemis を使え、ルーク

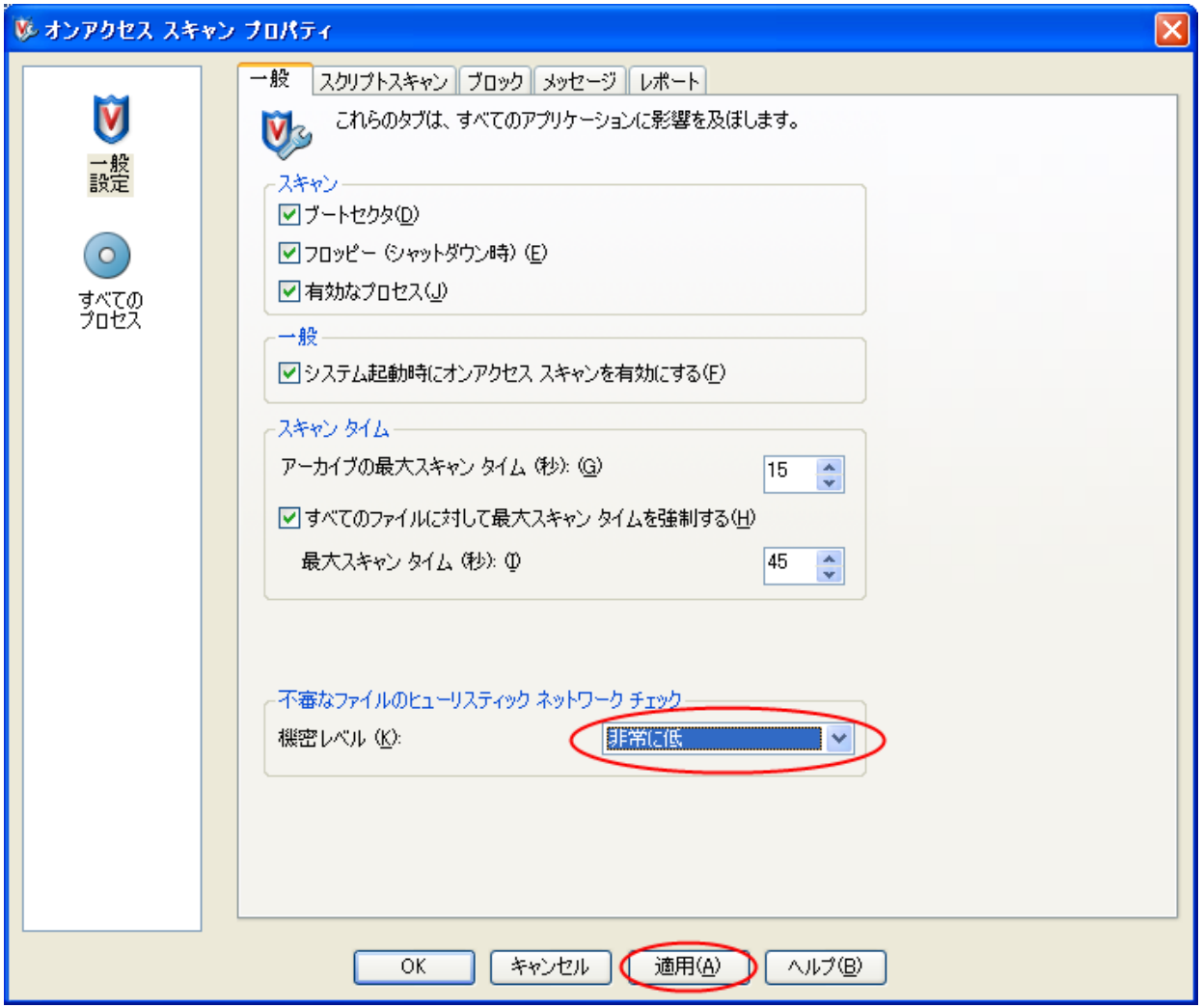
from “STAR WARS Episode IV”

McAfee Artemis Technology

- クラウドベースのサービス
- 疑いのあるファイルが確認された場合、Artemis はデータベースサーバにDNS要求を送信。サーバはそのプログラムが悪意のあるファイルか否かを確認し応答
- 一般消費者向けの製品では「Active Protection」として搭載

http://www.mcafee.com/japan/security/gti_artemis.aspより、一部改変して掲載

McAfee Artemis Technology



Artemis を有効化すると……

- 「非常に低」（次回のDATと同等の検出）では発見できない事例多数
  - VSE 8.7i patch 2 同梱版でのデフォルト設定
- 「低」（今後DATに追加予定のファイルの検出）にすると、とたんに発見できた事例を複数確認
  - 個人的にはこれを推奨中
- 「中」「高」「非常に高」に設定しても、検出率的にはあまり変わらないような気が……

Artemis はいつも君と共にある

……ネットにつながっていれば

from “STAR WARS Episode IV”

質問？