Практика реагирования на компьютерные инциденты

СТОЯНОВ РУСЛАН

РУКОВОДИТЕЛЬ ОТДЕЛА РКИ

KASPERSKY lab

ОСТОРОЖНО


VIOLENCE


PARENTAL
ADVISORY
EXPLICIT CONTENT


18+


DISCRIMINATION


@*!
BAD LANGUAGE


FEAR

Хроника «скорой помощи»

2015 год:

- Март – 10 млн , 4 выезда
- Апрель – 30 млн, 2 выезда
- Май – 2 выезда
- Июнь – 20 млн, 2 выезда
- Июль – 6 выездов,
- Август – 500 млн, 2 выезда
- Сентябрь – 8 выездов
- Октябрь – 100 млн, 2 выезда
- Ноябрь – 1 выезд

Первичные действия

Сначала узнать:

- Что случилось?

Далее выяснить:

- Структуру сети (сегментация, выход в в интернет)
- Политика ведения журналов событий
- Временные рамки происшествия
- Аномалии и признаки инцидента
- Идентификация

-> Аномалии и признаки инцидента
-> Группа
-> Вредоносное ПО, командные центры

Оперативный reverse engineering

Поиск ВПО производится с учетом:
- Временного интервала
- Аномалий и признаков

Далее:
- Построение файлового таймлайна (R-Studio)
- Логи за период времени инцидента (eventvwr.msc)
- Подозрительные соединения (tcpview, netstat)

Когда нашли:
- Изучение памяти (RAM Capturer, LiME, Volatility)
- Поиск инжектов кода
- Снятие обфускации, шифрования (вручную, с помощью эмулятора, удаленной **тестовой** машины)
- Поиск адресов командных центров
- Какие следы оставляет?
- По следам – скрипт
- Скрипт – на все компьютеры сети

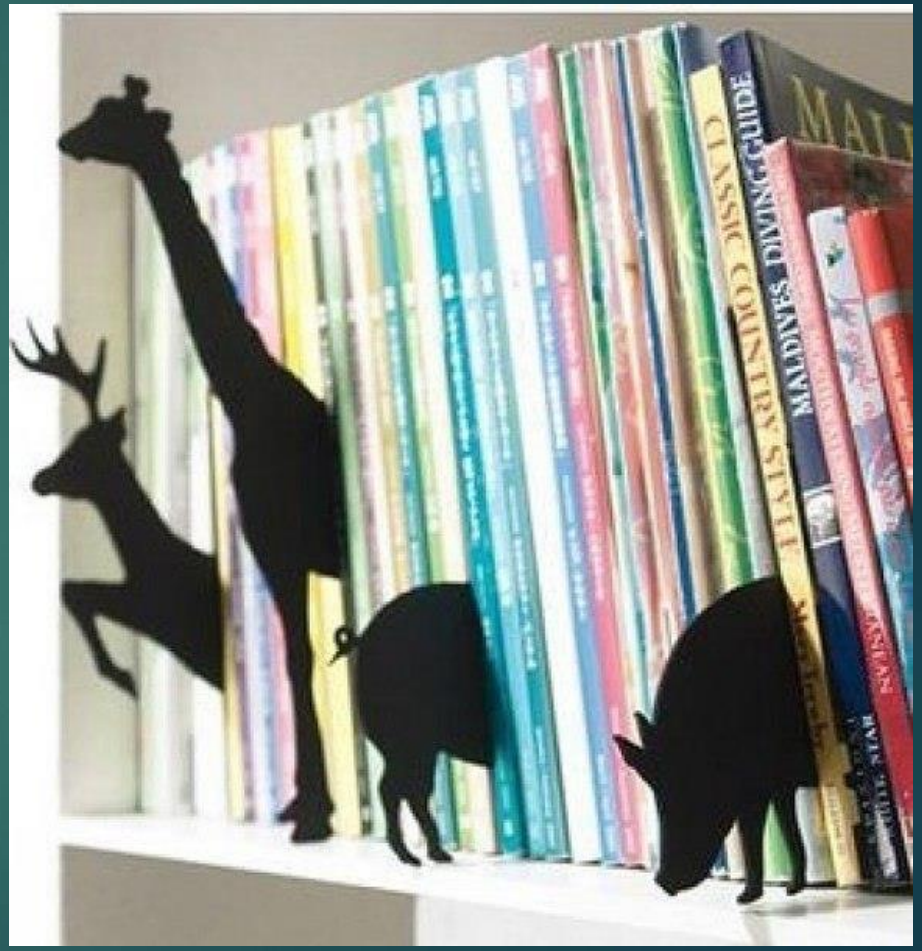
Поиск закладок

Создаются вручную.
Найти сложнее чем, следы трояна.

Поиск начинается с проверки стандартных вариантов:

- Протрояненный ssh
- Вебшелл
- Всевозможные туннели (в т.ч. средства удаленного доступа)
- Подозрительные учетные записи
- И т.д.

Поиск осуществляется на основе уже полученной информации (CC, почерк)



Идеальные админы

- Могут запустить скрипт на всех машинах
- Могут выгрузить любые логи за любой период (с контроллера домена, с прокси, IDS и т.д.)
- Имеют схему сети
- Быстро могут найти компьютер по его имени / ip-адресу
- Знают его предназначение
- Не ругаются на антивирус
- Сами предлагают заказать пиццу

Что не так?

- По бумагам – full compliance, на практике по-другому
- По бумагам – закуплено дорогостоящее железо, но настроено плохо
- По бумагам – есть антивирус, но устаревшей версии, с устаревшими базами, важные модули отключены
- Даже обновленный антивирус не спасает от APT

Пора переходить от бумажной безопасности к практической

Что делать?..

- Консолидация
- Частно-государственное партнерство
- Сотрудничество
- Оперативный обмен информацией
- Своевременное обращение
- Связка: ОРКИ – финцерт – компании – органы
- В этой связке проведены расследования инцидентов и задержания преступников