

Как взломать сервер Браузером и ...Зеброй

Или
Трилогия о Троянской Зебре

By Leon Maister
Feb 2014

Часть 1

АТАКА

Как это было...

Интернет-злоумышленники, назвавшие себя хакерским объединением Group-XP из Саудовской Аравии, обнародовали в интернете личную информацию нескольких тысяч израильтян, сообщает газета "Гаарец".

В понедельник, 2 января, хакеры взломали израильский сайт [one.com](#) публикующий новости спорта, и установили на нем [Pastebay](#). На этом сайте взломщики разместили копии баз данных с базами личных данных, включая имена, фамилии и номера удостоверений личности и кредитных карт.

Саудовские хакеры выложили в Сеть данные тысяч израильтян

Саудовские хакеры выложили еще 11.000 кредиток

19:54

яря 2012 г., 10:29



... опубликовали в интернете 11.000 израильских кредитных карт. Банк Израиля сообщил, что проверяет



Хакеры из Саудовской Аравии выложили в Сеть данные тысяч израильтян, сообщает газета "Гаарец".

... кредитных карт по меньшей мере 400 ведущих израильских кредитных карт.

Саудовские хакеры атаковали сайты больниц "Асута" и "Шива"



Интернет-сайты ведущих израильских больничных центров "Асута" и "Шива" вернулись к нормальной работе после сегодняшней атаки саудовских хакеров, информирует радиостанция "Коль Исраэль". Отмечается, что в данный момент доступ на сайты "Асута" и "Шива" все еще невозможен с иностранных ip-адресов. Программисты опасаются повторения сетевой атаки на известные медицинские ресурсы.

Пострадавшие от хакеров оценили ущерб в 1,3 млрд шекелей
В окружной суд Тель-Авива подан групповой иск против компании Cal ("Картисей-ашраи Исраэль" - "Израильские кредитные карты") - в 1,3 млрд шекелей.
ущерб в 770 шекелей и общий ущерб всем клиентам компании - в 1,3 млрд шекелей.

Разбор Полетов ...и Выводы

Любая уязвимость будет использованна злоумышленниками для причинения максимального ущерба

Часть 2

ТРОЯНСКАЯ ЗЕБРА

**Данная демонстрация
включает в себя уязвимости
из живых систем,
консолидируемых в единую
апликацию**

Часть 3

ОХОТА НА ЗЕБРУ

Итак, как защитить аппликацию?

- **WAF**
- **Pen Testing**
- **DAST**
- **SAST**
- **Combine***

Концепция SDLC

**Ключевым условием
надёжности приложения является
*внедрение решения по
безопасности*
в живой цикл разработки продукта**

Эксплуатация: Установка и Настройки

- **Установка**
 - *Легкость*
 - *Минимальные ресурсы*
 - *Минимальное время*

- **Настройки**
 - *Простота*
 - *Гибкость*

Статический Анализ Кода

- Сканирование

- *Интеграция в среду разработки*

- *Широкий список сканируемых языков*

- *Широкий список фреймворков*

- *Полнота и точность результатов*

- Максимальное количество найденных уязвимостей

- Минимальное количество ложных срабатываний

Обзор Результатов

- Векторы атак на исходном коде
- Документация по уязвимостям
- Рекомендации по устранению уязвимостей

Отчеты

- Гибкость в генерации отчета
- Выбор удобного формата отчета
- Полнота информации
- Фильтрация и консолидация результатов в зависимости от настройки

About Us



- **Israeli Company**
- **Tel Aviv**
- **Since 2006**
- **CTO – Maty Siman**
- **Leading SAST Vendor**
- **On Premise and on Demand offering**
- **Hundreds of customers and service providers worldwide**
- **Named “Visionary” & “Cool Vendor” by Gartner**
- **Patented Technology**



Благодарю за внимание!

Вопросы?

www.checkmarx.com