Контроль внешнего периметра
-
простые решения, максимум эффективности

Евгений Зайцев
независимый эксперт

Почему?

1. Внешний периметр компании - доступен всем
2. Уязвимости будут всегда
3. Современный хакерский инструментарий существенно снизил порог входа в “профессию”
4. Современный “хактивизм” - это бизнес, это выгодно, это модно

Массовая культура: фильмы

Крепкий орешек 4.0

Джон МакКлейн ловит хакера-нигилиста, пытающегося обрушить экономику США

Матрица

Первая часть знаменитой трилогии сестер Вачовски: хакер Нео узнает, насколько глубока эта кроличья нора

Начало

Навороченный триллер Кристофера Нолана про вора, проникающего в мозги людей

Хакер

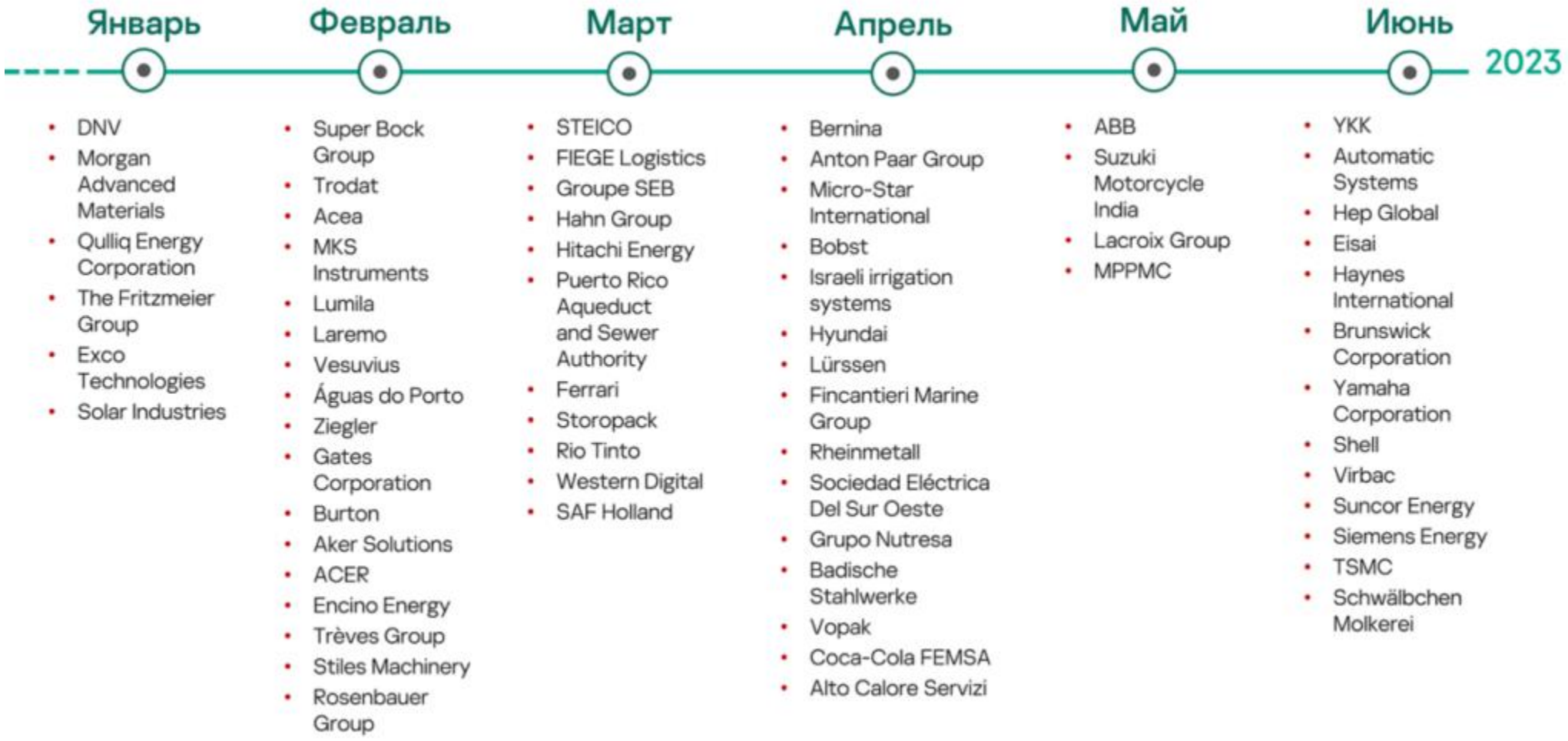
Американское правительство пытается обуздать погоду

Хакеры

Команда университетских компьютерных гениев вступает в войну с сетевым злодеем.

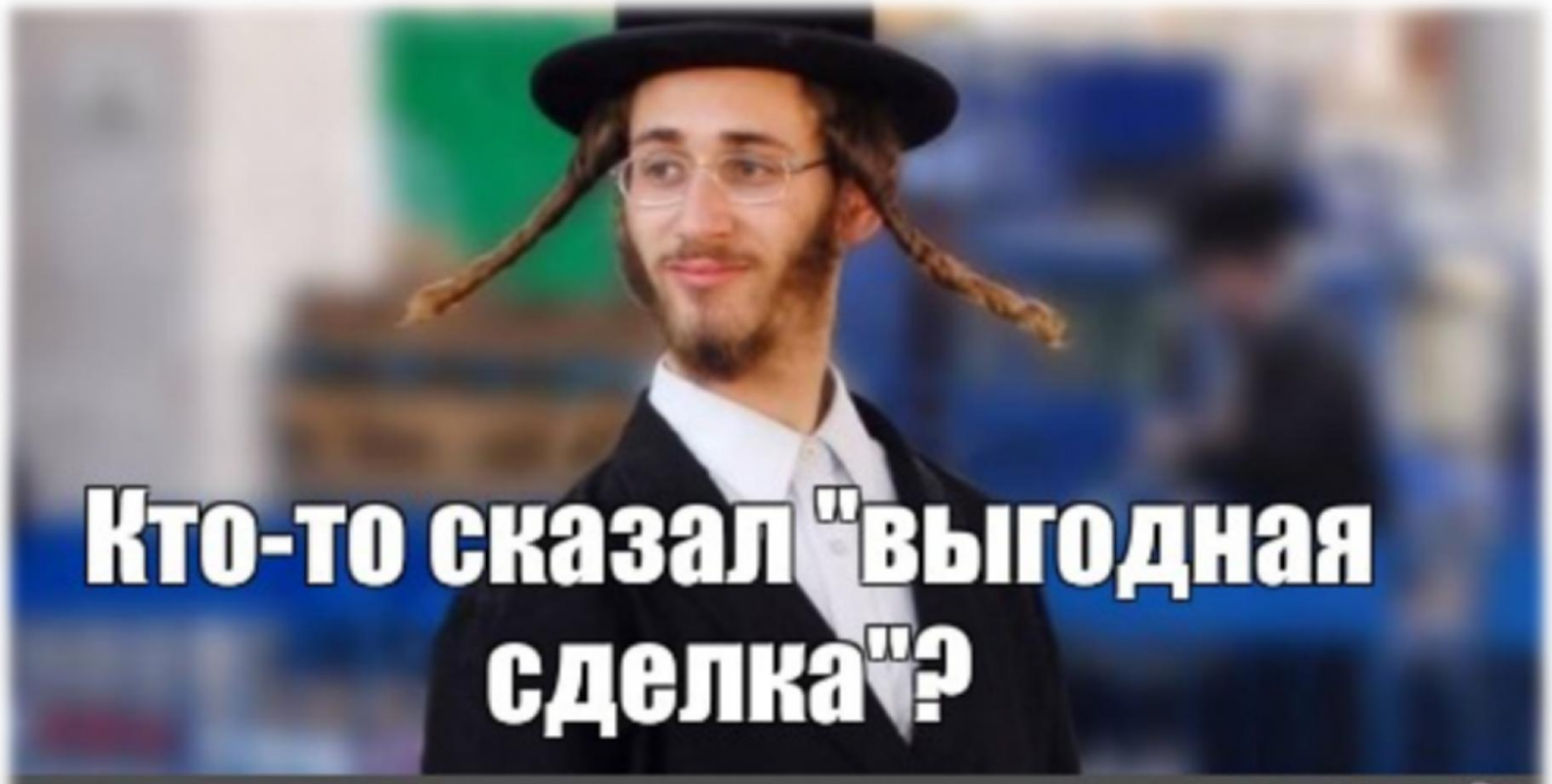
Массовая культура: игры

Их взломали внешние злоумышленники



Дебет/Кредит

1. Стоимость выкупа у злоумышленников - от 0,3 млн. $
2. Ущерб от инцидента - обычно в 10 раз больше...
3. Затраты на контроль вн. периметра - от 0,012 млн. $/г.



Зачем?

- Снижаем нашу привлекательность для хакера
- Приводим инфраструктуру к контролируемому состоянию
- Тратим меньше денег работодателя, проще обосновать
- Проще обосновываем свои KPI, больше зарабатываем

Делаем раз

1. Инвентаризация, выясняем что нам принадлежит:
   – IP-адреса, подсети, домены, порты, сервисы.
   – зачем существует, в чьих интересах, кто ответственный.
2. Закрыть все ненужное.
3. По завершении п.2 повторить п.3.

Делаем два

- Искать уязвимости по результатам инвентаризации:
  - уязвимости веб-приложений
  - уязвимости системных служб
- Обосновать необходимость устранения
- Поставить сроки устранения
- Проконтролировать устранение

Делаем три

1. Устаем ругаться и доказывать, пишем и согласовываем политики, регламенты и т.д.
2. Не забываем вписать все это в KPI и не только себе!!!
3. Устаем от ручного труда, делаем автоматизацию

PROFIT!

Чем?

1. OpenSource - условно бесплатно, требует больших интеллектуальных затрат на сопровождение
2. Готовые сервисы - относительно дешево, сердито, неодинаково по качеству.
3. Купить инхаус решение - дорого, неодинаково по качеству, требует интеллектуальных затрат на сопровождение
4. Подписаться на канал @avleonovrus

Спасибо хакерам за наше сегодня

А вам спасибо за внимание!

По вопрсам, с пожеланиями и угрозами обращаться:

evgeny.zaitsev@gmail.com