ЭЛВИС-ПЛЮС

Уязвимости современных КИС

Практические примеры или просто о сложном

Юдаков Антон
Ведущий инженер Технического департамента
ОАО «ЭЛВИС-ПЛЮС»

17.10.2012

ЭЛВИС-ПЛЮС

Уязвимости современных КИС

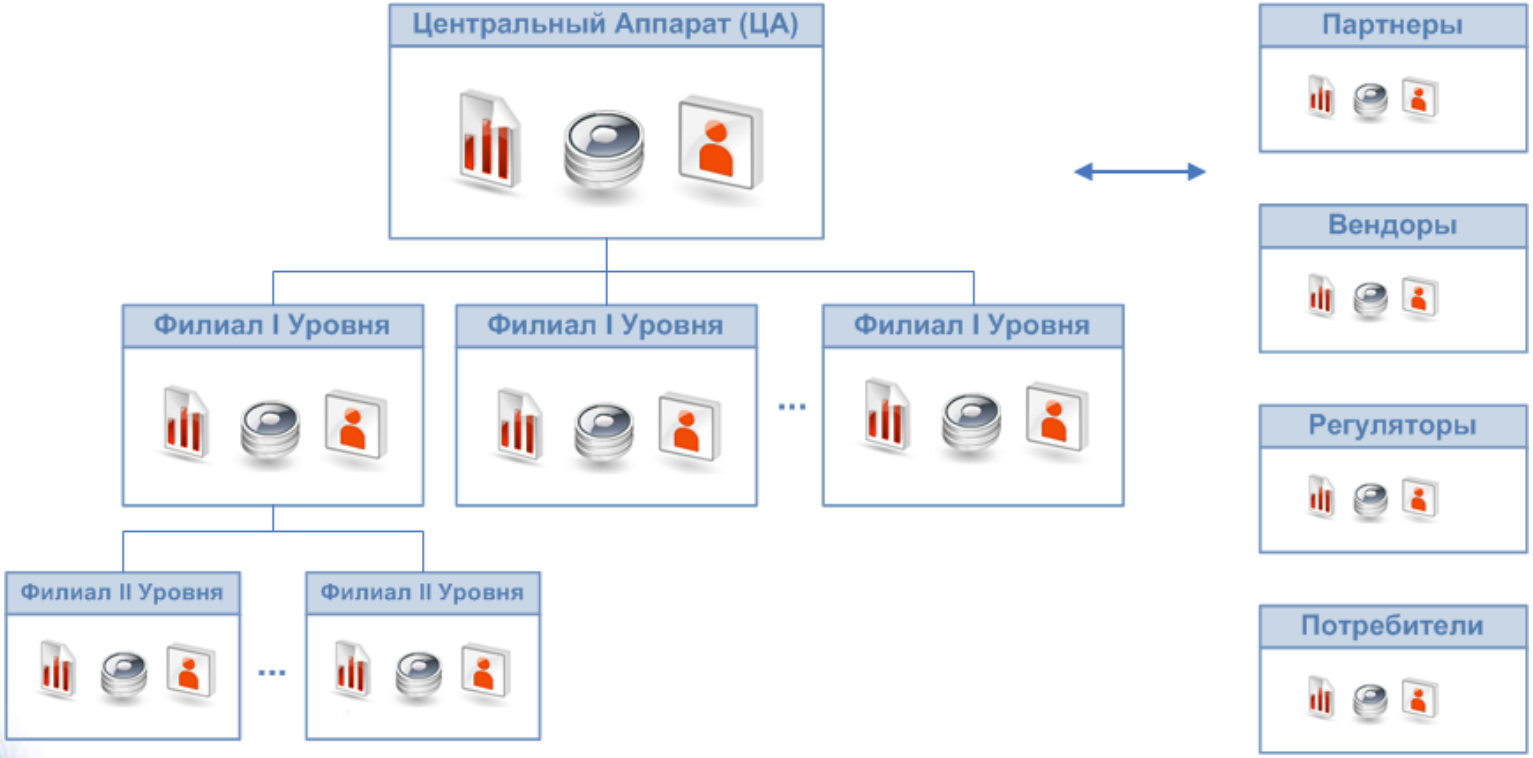
Вопросы презентации

- Общий взгляд на современную КИС
- Уязвимости и атаки – реальная ситуация
- Возможные методы – практические примеры:
  - USB эмуляторы HID-устройств
  - туннелирование трафика
- Что вам с этим делать?

ЭЛВИС-ПЛЮС

Общий взгляд на современную КИС

КИС Enterprise-уровня



Общий взгляд на современную КИС

КИС Enterprise-уровня, уточнение

Будем считать, что в части вопросов обеспечения ИБ вы достигли высокого уровня зрелости, в т.ч. в вашей КИС:

- внедрены и используются различные подсистемы ИБ;
- на серверах и АРМ устанавливаются обновления безопасности, причем не только для ОС и MS Office;
- пользователями и администраторами используются сложные пароли или двухфакторная аутентификация;
- и т.д.

Общий взгляд на современную КИС

КИС Enterprise-уровня, уточнение

Если это не так, например:

- у вас нет антивирусного ПО (!?), либо его использование не централизованно;
- администраторами используется один (общий!?) пароль для управления всеми серверами/системами и он не соответствует определенной в Компании политике паролей;
- не устанавливаются обновления используемого ПО, (например, Adobe Reader!?);
- и т.д.

Знайте – вас легко взломать, возможно, это даже уже произошло. Просто на самом деле вы об этом еще не знаете.

ЭЛВИС-ПЛЮС

Уязвимости и атаки – реальная ситуация

Факты за 2009-2012 гг.

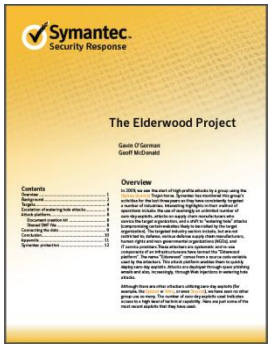
Эти компании были взломаны.

В продолжения необходимости обобщить причину и способы взлома появился термин APT – Advanced Persistent Threat (Постоянные прицельные атаки).

ЭЛВИС-ПЛЮС

Уязвимости и атаки – реальная ситуация

Факты за 2009-2012 гг., уточнение


Symantec.
Security Response

The Elderwood Project

Gavin O'Gorman
Geoff McDonald

Contents

Overview

The Elderwood Project:

- Цели: предприятия оборонной промышленности, предприятия электроэнергетики, предприятия различных отраслей промышленности, финансовые, страховые и телекоммуникационные компании (в различных странах).
- Возможные мотивы: кража интеллектуальной собственности, планов, контактов, информации об инфраструктуре, аналитика для дальнейших атак.

Источник: Symantec Security Response. The Elderwood Project

ЭЛВИС-ПЛЮС

Уязвимости и атаки – реальная ситуация

Результаты исследований

83%

Компаний считают, что становились целью атак APT

65%

Компаний считают, что не обладают ресурсами, чтобы им противостоять

91%

проникновений потребовали «часов» /«дней» на компрометацию КИС

85%

проникновений потребовали «недель» / «месяцев» на их выявление

Источник: Ponemon Institute Survey Conducted «Growing Risk of Advanced Threats»
Источник: Verizon 2011 / 2012 Data Breach Investigations Report

ЭЛВИС-ПЛЮС

Уязвимости и атаки – реальная ситуация

Advanced Persistent Threats - APT

APT!

- Технологии стали сложнее, порог вхождения в «хакерство» ниже, опасность взлома выше.
- Много нового в нападении, мало – в защите.
- Эволюция взломов: ради забавы, ради наживы, ради стратегического доминирования.

APT!?

- Все APT-взломы по сути набор тех же самых атак, что мы знали раньше?

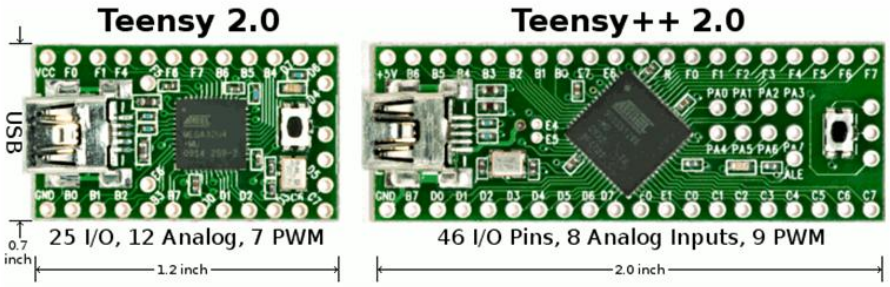
Уязвимости современных КИС

ПРИМЕРЫ?

Методы – практические примеры

1. USB эмуляторы HID-устройств

Teensy USB Development Board



Key Features:

- USB can be any type of device
- AVR processor, 16 MHz
- Single pushbutton programming
- Easy to use Teensy Loader application
- Free software development tools
- Works with Mac OS X, Linux & Windows
- Tiny size, perfect for many projects
- Available with pins for solderless breadboard
- Very low cost & low cost shipping options

Specification	Teensy 2.0	Teensy++ 2.0
Processor	ATMEGA32U4	AT90USB1286
Flash Memory	32256	130048
RAM Memory	2560	8192
EEPROM	1024	4096
I/O	25	46
Analog In	12	8
PWM	7	9
UART,I2C,SPI	1,1,1	1,1,1
Price	$16	$24

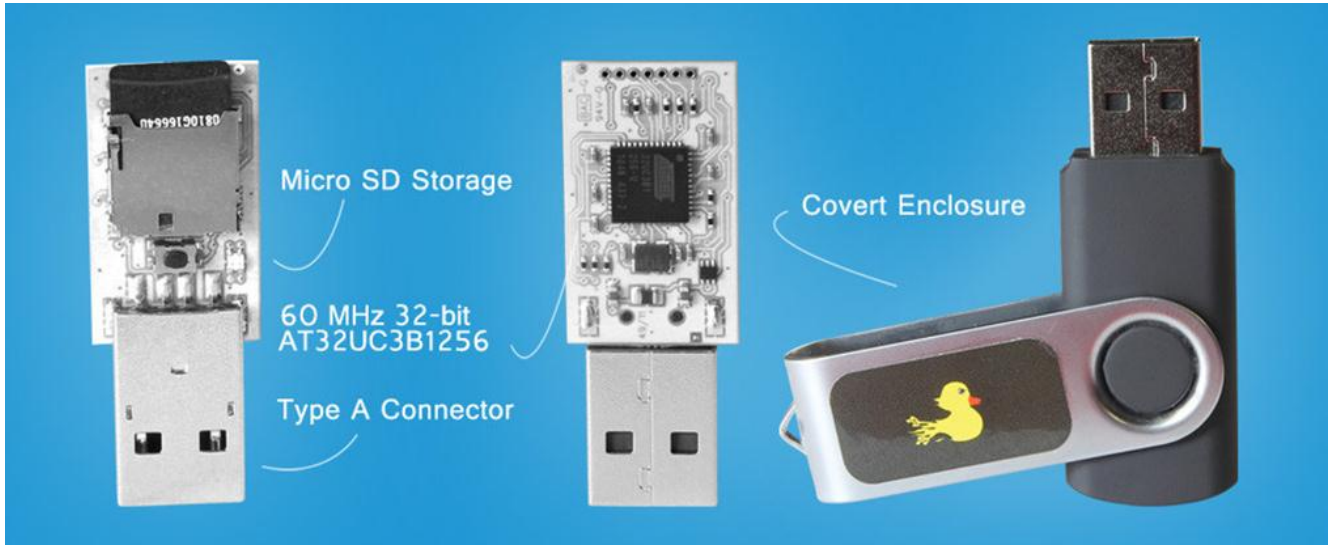
Это программируемые микроконтроллеры, цена:

$16 или **$24**

Могут эмулировать клавиатуру, фактически позволяют выполнить код в обход средств защиты!

Методы – практические примеры

1. USB эмуляторы HID-устройств



Можно купить готовое к использованию устройство в виде USB-flash накопителя (работающего!)

Методы – практические примеры

1. USB эмуляторы HID-устройств

*Кстати, на распродаже всего за **$59,99!***

Методы – практические примеры

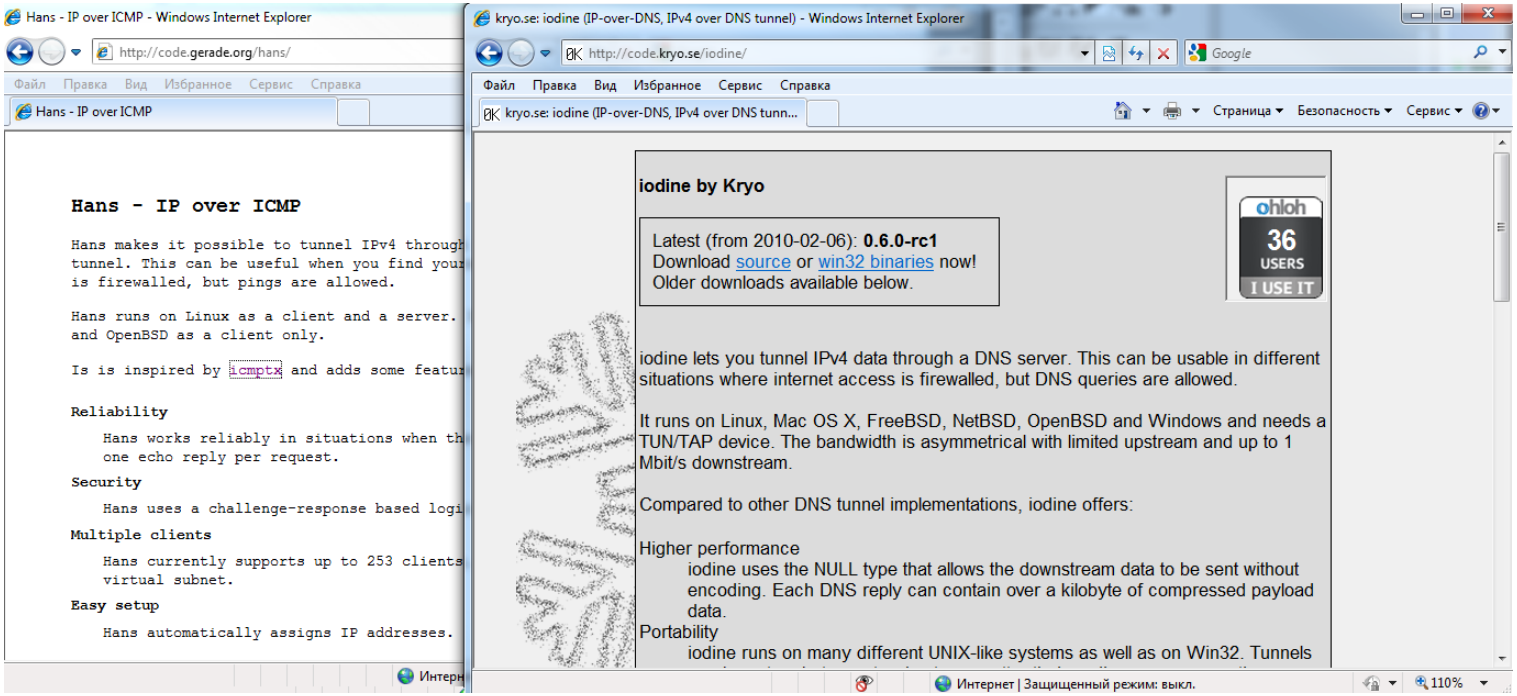
Вспомним Duck test / Утиный тест

Если оно выглядит как утка, плавает как утка и крякает как утка, то это, вероятно, утка и есть.

If it looks like a duck, swims like a duck and quacks like a duck, then it probably is a duck.

Методы – практические примеры

2. Туннелирование трафика

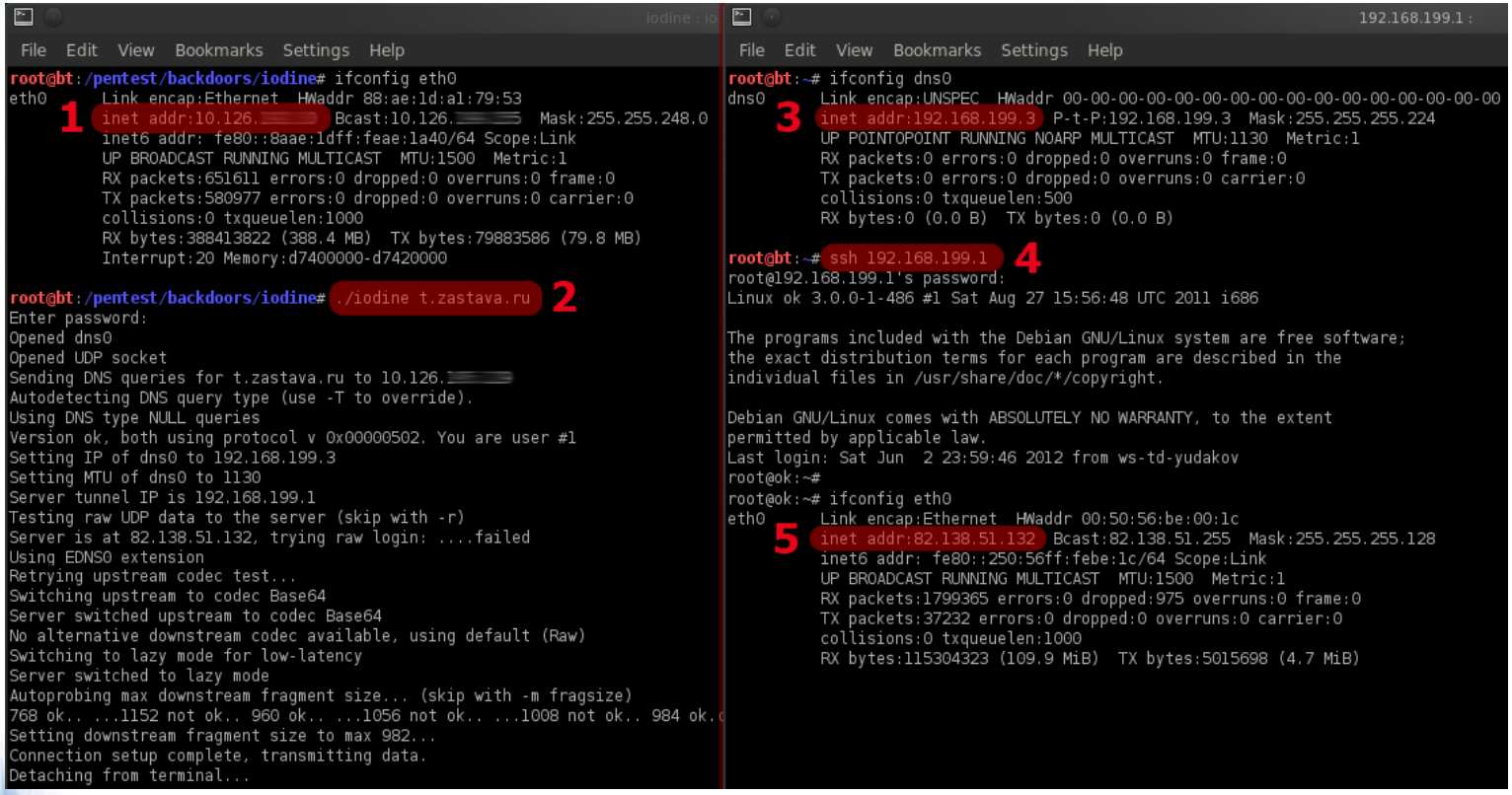


Сайты известных утилит –
Hans (ICMP-туннелирование) и Iodine (DNS-туннелирование)

ЭЛВИС-ПЛЮС

Методы – практические примеры

2. Туннелирование трафика



Пример организации DNS-туннеля для доступа к внешнему серверу из изолированного сегмента КИС

Методы – практические примеры

2. Туннелирование трафика

Если вы думаете, что доступ к сети Интернет ограничен и невозможен в обход используемых средств ограничения доступа, проверьте:

- ping 8.8.8.8
- nslookup google.ru

Если вы получили ответ – **доступ к сети Интернет возможен!**

Уточнение – **возможен доступ и из сети Интернет к вам!**

ЭЛВИС-ПЛЮС

Уязвимости и атаки – реальная ситуация

Advanced Persistent Threats – APT, уточнение

- Все «APT-взломы» это набор тех же самых атак, что мы знали раньше (уязвимости, эксплоиты; то же туннелирование трафика – активно использовалось ранее).

- Что нового привносит APT, о чем я раньше не знал? Что нового должен делать, чего раньше не делал?
  - помимо готовности противостоять APT-атакам – максимально сокращать время на выявление/разбор инцидентов ИБ.
  - не забывать про обучение пользователей!

Что делать?

- Если вы знаете, что вопросы/проблемы обеспечения ИБ в КИС вашей Компании далеки от закрытия – закрывайте их.
- Если вы считаете, что уже сделали это – проверяйте (Pentest).
- Если вы уверены в должном обеспечении ИБ в КИС вашей Компании, вы регулярно заказываете тесты на проникновение, у вас построен / работает SOC и вы считаете, что готовы противодействовать APT-атакам – просто проверьте насколько вы защищены от способов и средств, рассмотренных в примерах:
  - USB эмуляторы HID-устройств
  - туннелирование трафика

ЭЛВИС-ПЛЮС

Спасибо за внимание!

Юдаков Антон
Ведущий инженер Технического департамента
ОАО «ЭЛВИС-ПЛЮС»

тел. (495) 276-02-11
e-mail: a.yudakov@elvis.ru
http://www.elvis.ru