Угрозы в Интернете

Филипп Роггебанд, менеджер по развитию бизнеса

группа «Сети без границ», страны с развивающейся экономикой

Вопросы к обсуждению

- Отчет по безопасности Cisco за 2009 г.
- Угрозы в Интернете
- Защищенные сети без границ
- Вопросы и ответы

Насущные задачи
Противоборствующие силы

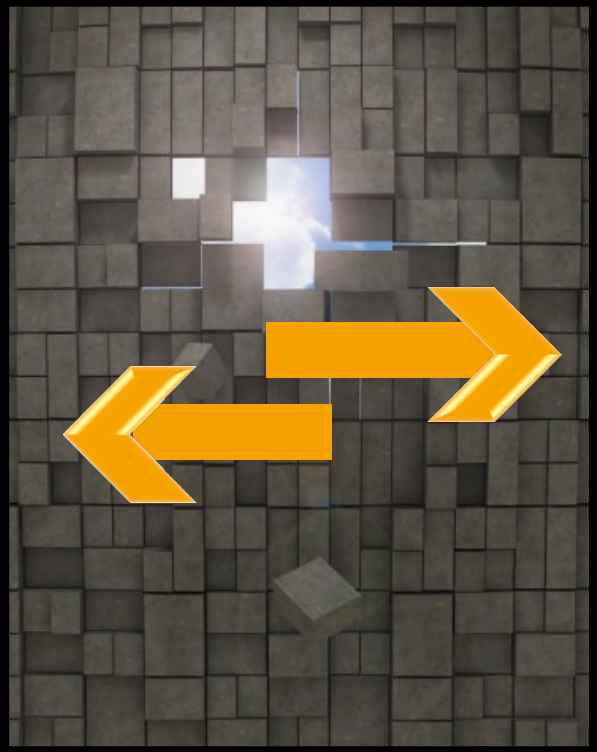
Глобализация

Мобильность

Совместная работа

salesforce.com

Корпоративное ПО как сервис



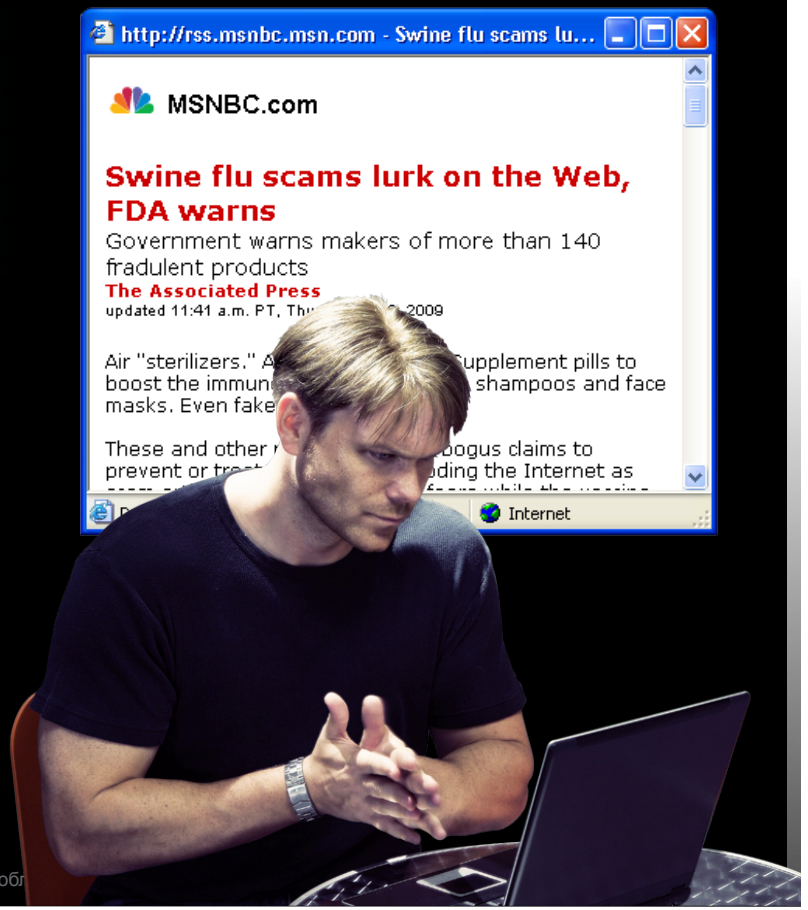
Угрозы

Допустимое использование

Утрата данных

Эволюция угроз безопасности

- Специализация преступников как фактор усложнения атак
- Веб-экосистемы как главное направление развития угроз
- Преступники злоупотребляют доверием пользователей, что ставит под сомнение традиционные средства защиты
- Творческий подход к привлечению жертв (бизнес-модели)

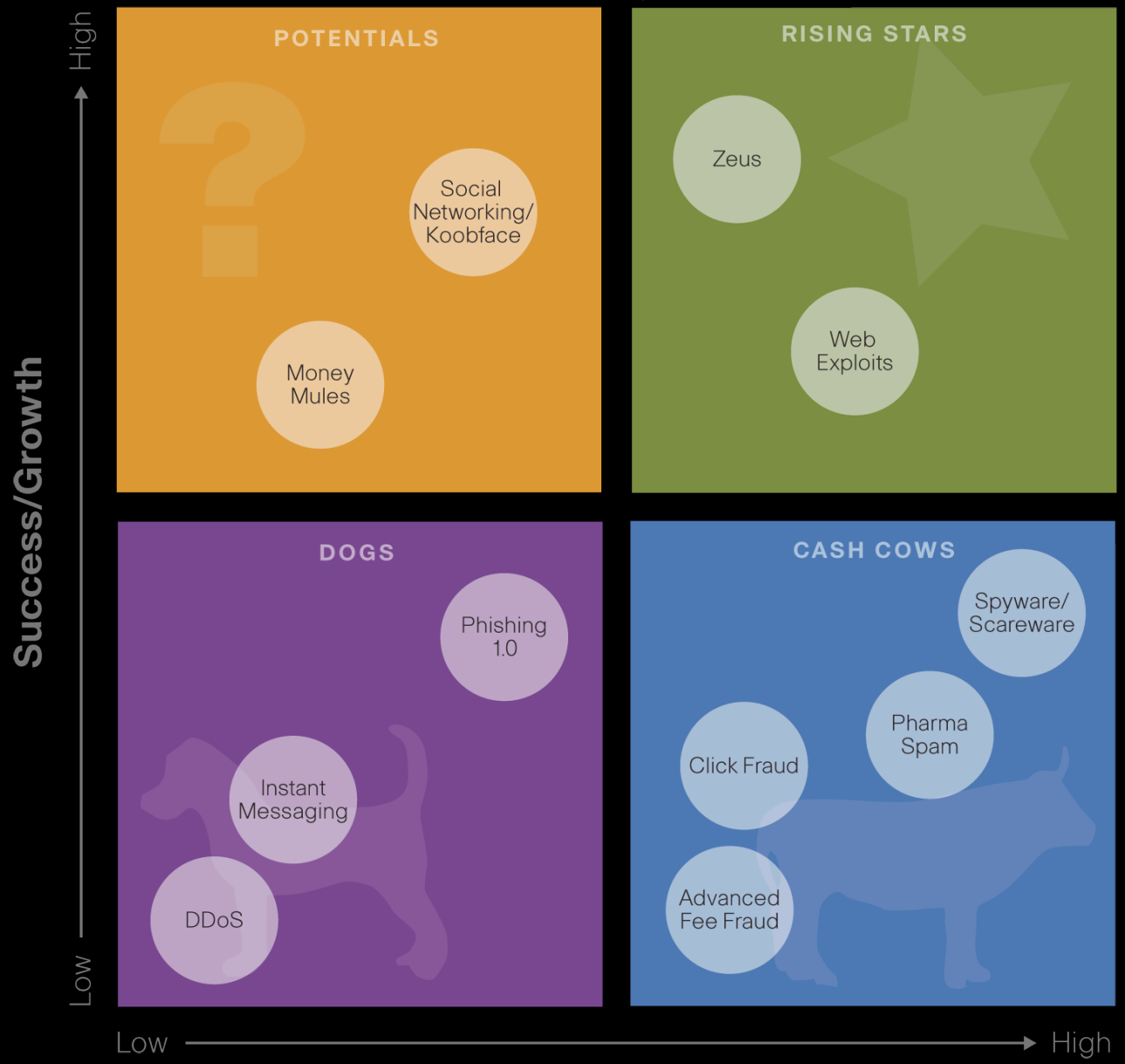


Отчет по безопасности Cisco за 2009 г.

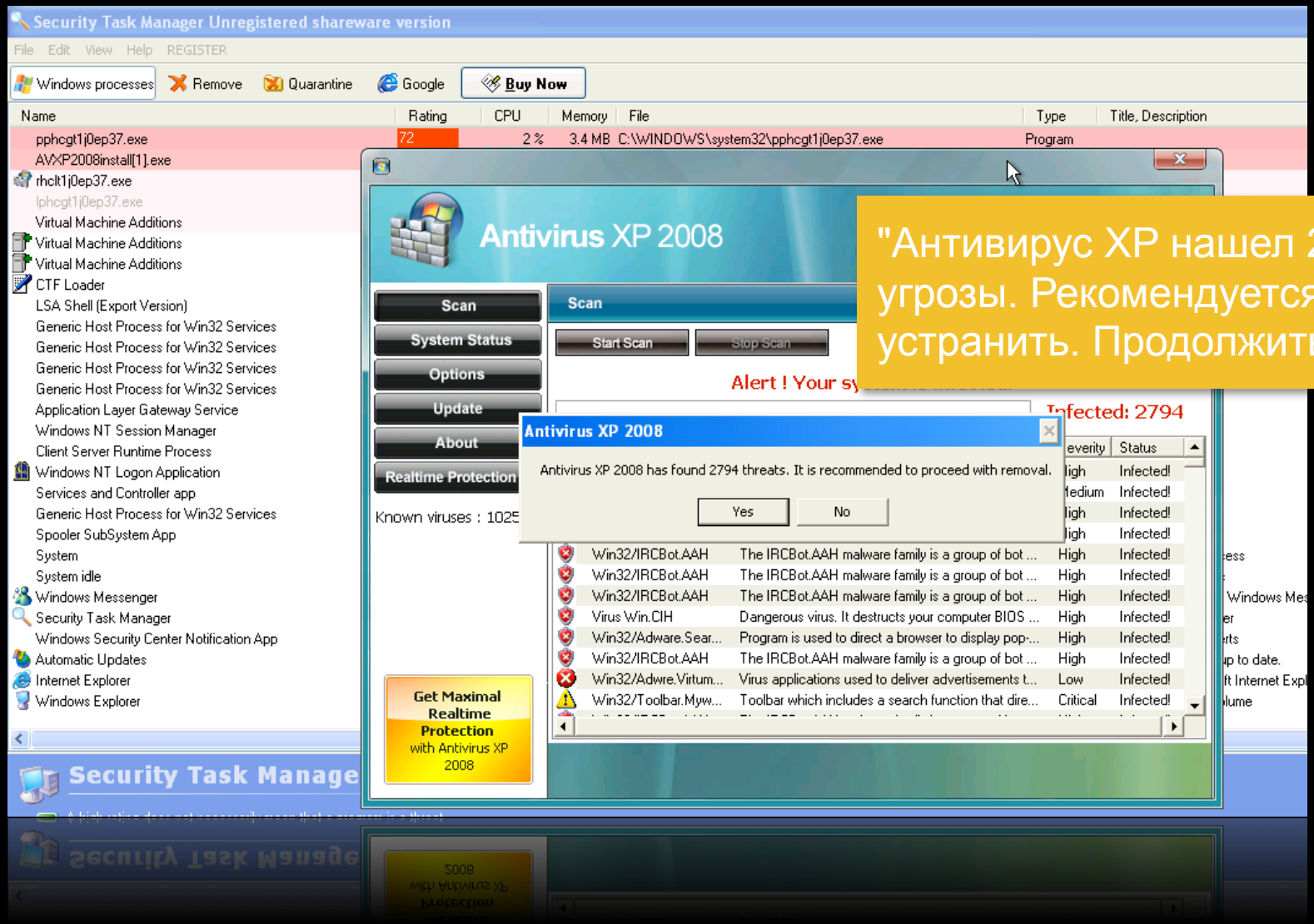
Содержание

- Социальные сети
- Риски при работе в Интернете
- Монетизация киберпреступлений
- Указатель ресурсов киберпреступности
- Номинации "образцово-показательные киберпреступления"

Матрица : доход на капитал, вложенный в киберпреступление

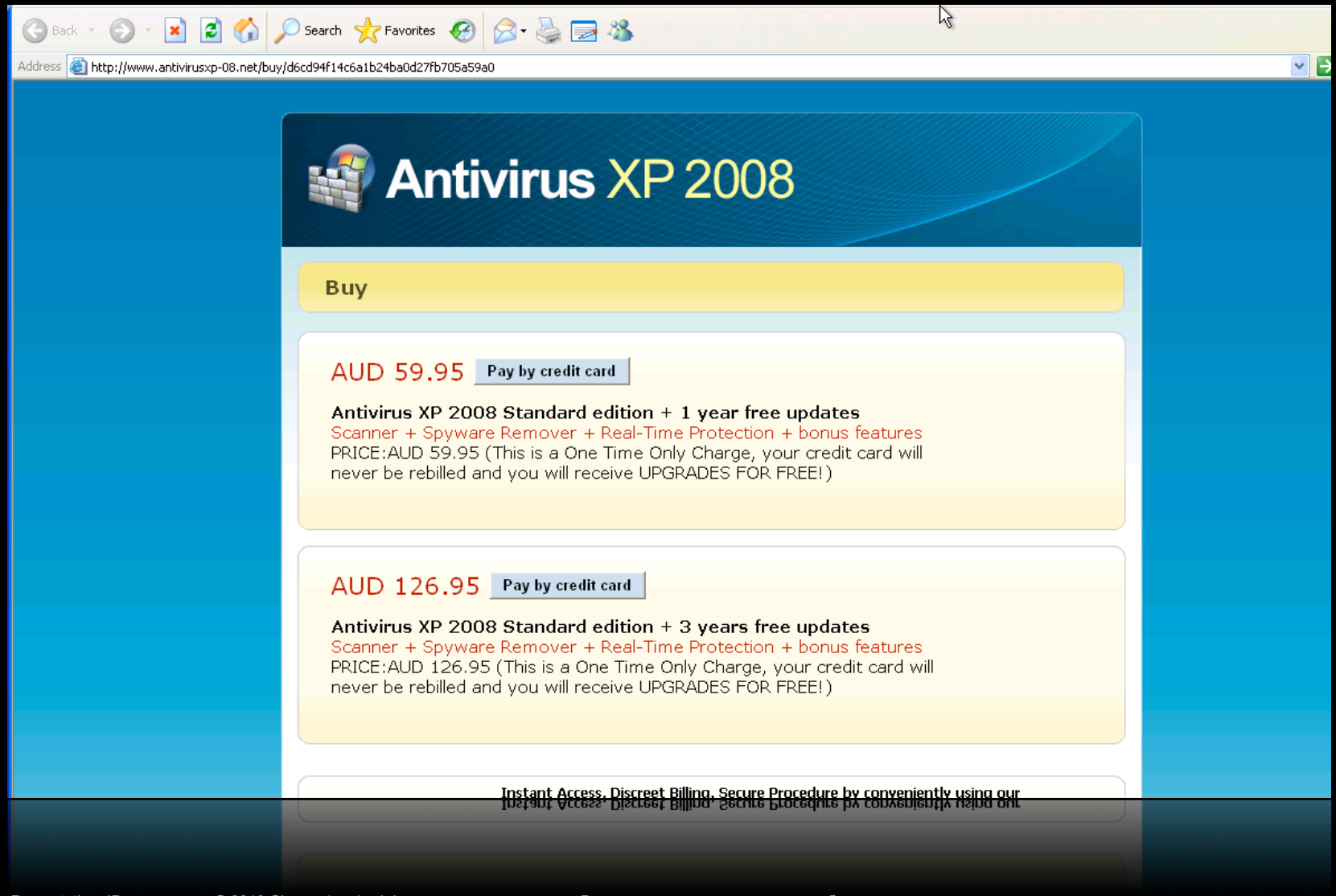


"Изделие года" в области киберпреступности



"Антивирус XP нашел 2794 угрозы. Рекомендуется их устранить. Продолжить?"

После сканирования – переход на узел, определяющий местонахождение и IP-адрес, удаление кнопки "Закрыть" с экрана



Bakasoftware управляет криминальной сетью

- Партнеры Bakasoftware по продаже "шпионского" ПО для “устрашения”
- Партнеры загружают "ПО-устрашитель" в ботсети
- Партнеры выплачивают Bakasoftware комиссионные за покупки клиентов
- Доход партнера № 2 за 10 дней – 147 тыс. долларов, за год – 5 млн.

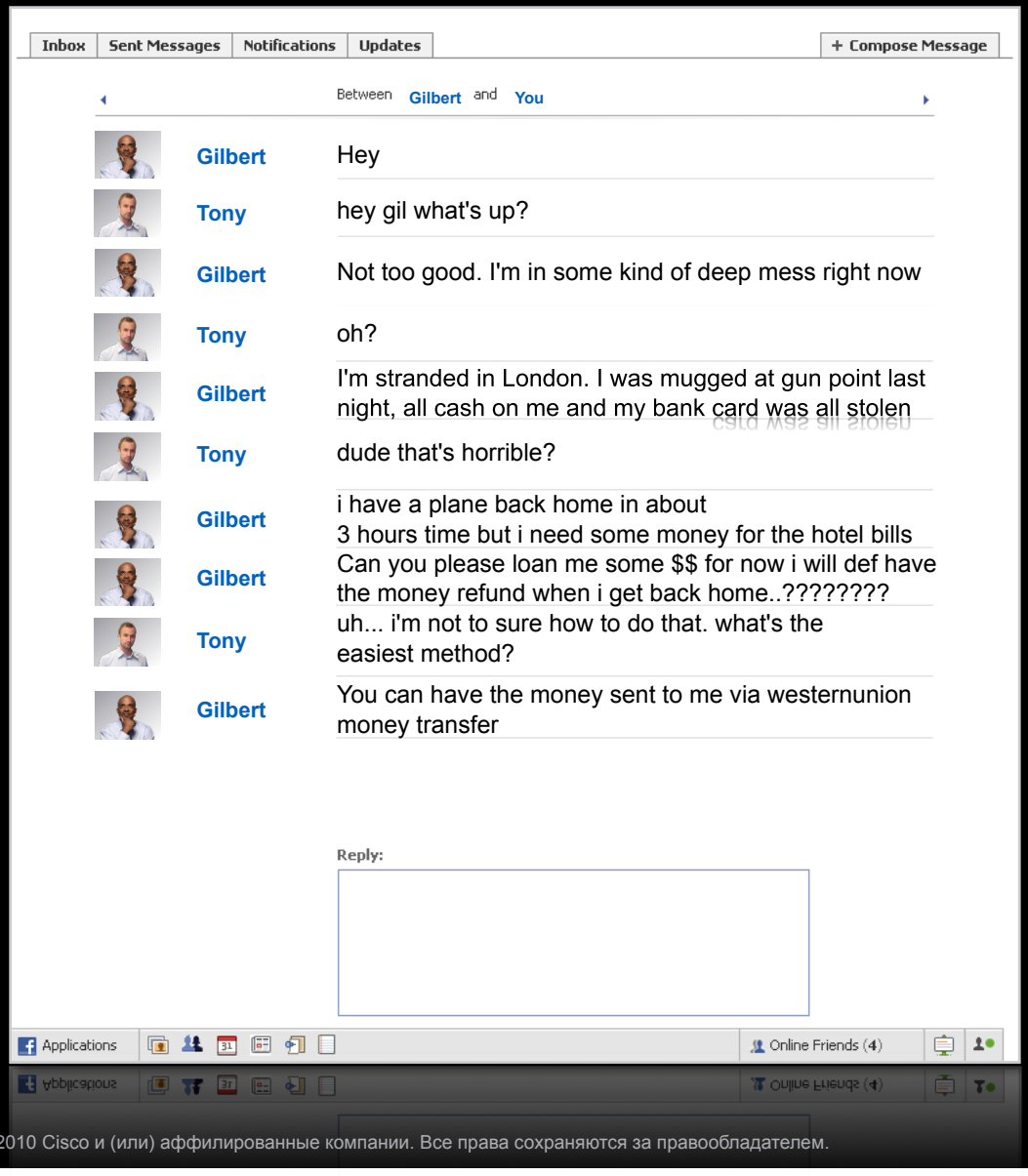
  154 825 установок, 2772 покупки

	Loader	Сетапы	Покупки	Покупки
День 1	37943	19989	667	29853.86
День 2	39895	19722	74	5420.64
День 3	41687	18619	384	28148.96
День 4	38059	16038	249	13908.24
День 5	39160	15335	176	9726.17
День 6	29968	12076	207	11672.71
День 7	13293	6866	129	6920.81
День 8	18055	8915	157	7557.25
День 9	29642	14802	265	12852.29
День 10	50457	22463	464	21055.29
Итого	338159	154825	2772	147116.22
	Loads	Installs	Purchases	Total

Панель Bakasoftware с доходами за 10 дней ДФ № 2

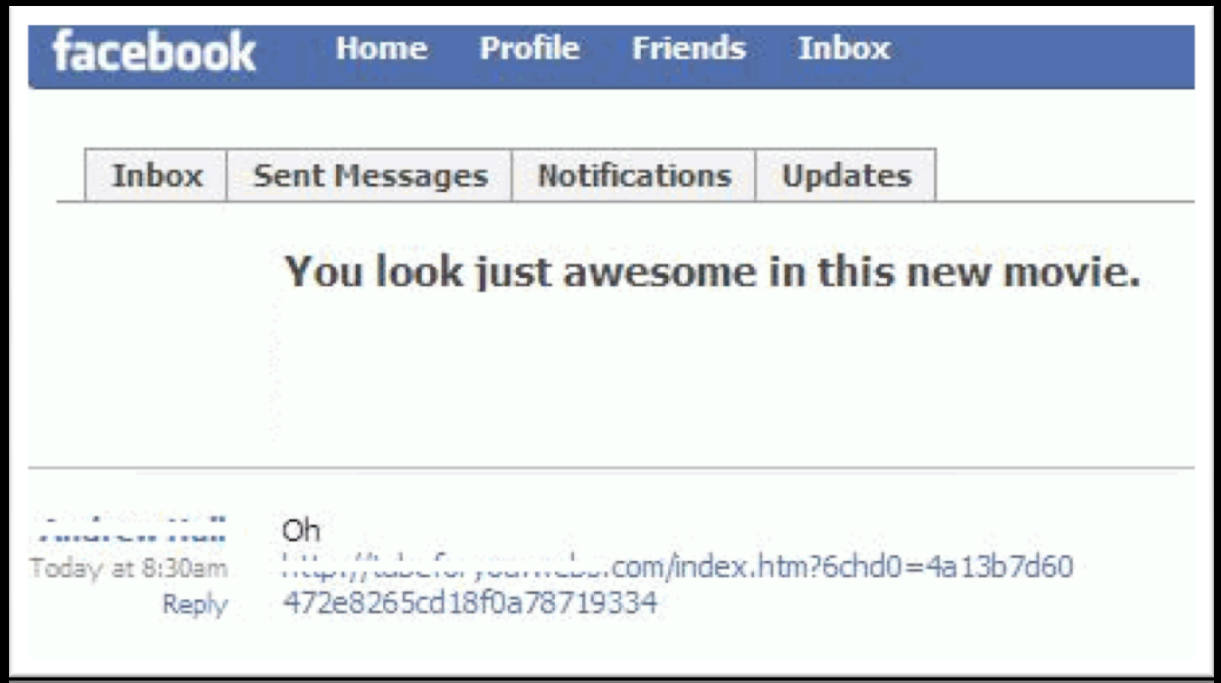
Источник: http://www.secureworks.com/research/threats/rogue-antivirus-part-2/?threat=rogue-antivirus-part-2

Атака на Веб 2.0 – чат с "другом"



Всё вместе: червь Koobface

- Ссылки передаются на взломанные учетные записи социальных сетей (или приходят с них)



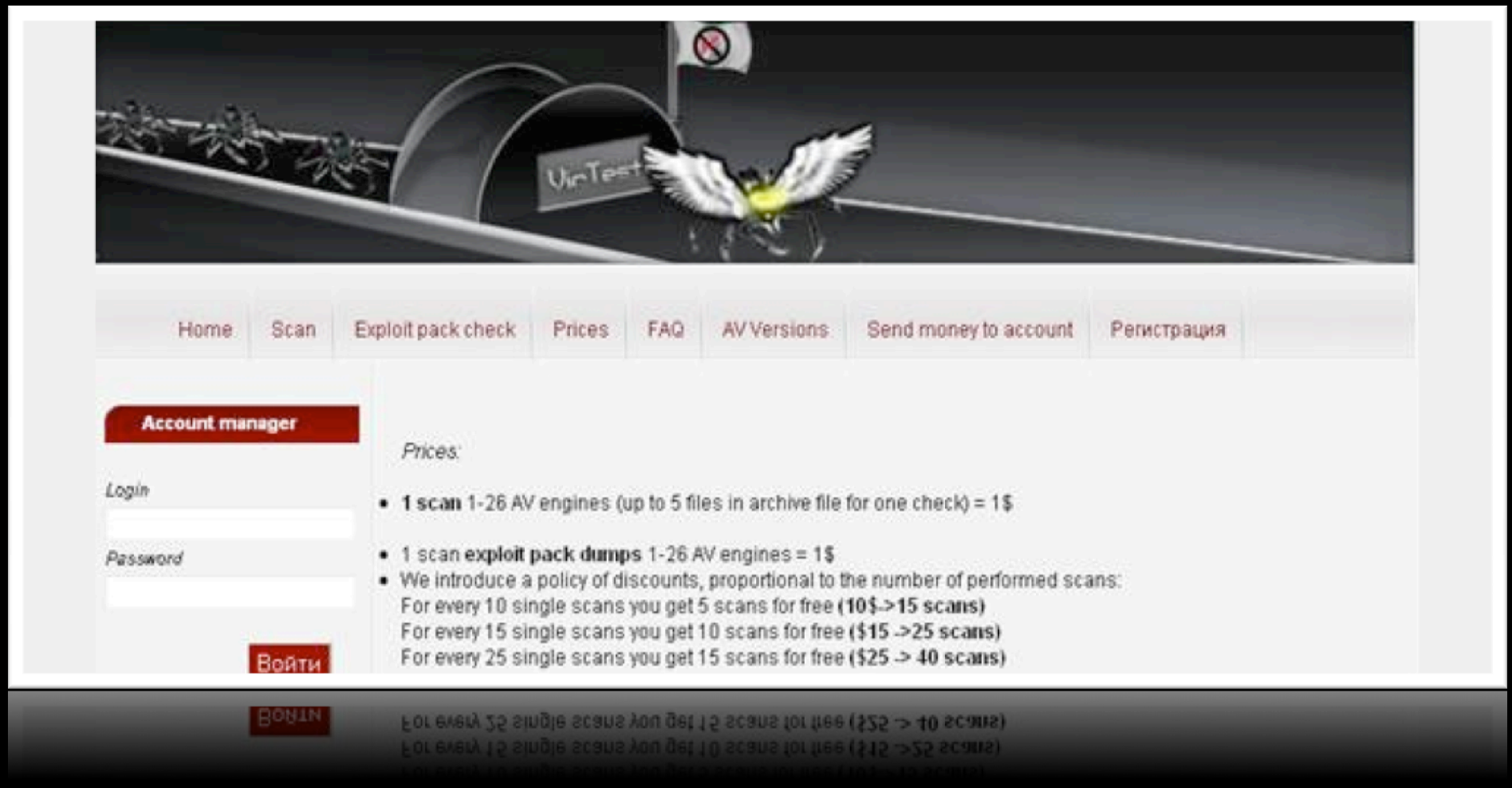
- Ссылка ведет к подложному узлу видео, где пользователю предлагают для просмотра установить новый проигрыватель Flash или кодек

Почему веб-эксплойт трудно обнаружить: BoingBoing.net: популярный блог

- URL в обозревателе: **1**
- Запросов HTTP Get: **162**
- Изображений: **66** из **18** доменов, в т.ч. **5** отдельных невидимых отслеживающих изображений 1x1 пиксель
- Скриптов: **87** из**7** доменов
- Куки-файлов: **118** из **15** доменов
- **8** Flash-объектов из **4** доменов

ПО как служба: все больше предложений от злоумышленников

Служба проверки вредоносного ПО на обнаружение с помощью антивирусов



Почему Zeus?

Основа конфигурационного файла Zeus

- По умолчанию Zeus ворует все поля формы в обозревателе
- Каждый контроллер ботсети может адаптировать хищение персональных данных

Steal from these brands

```
banesnet.banesto
*patagoniaebank.com
*inetnkp.adelaidebank
*login.commbank
*sydneycu.com
```

- Может указать, что не похищать

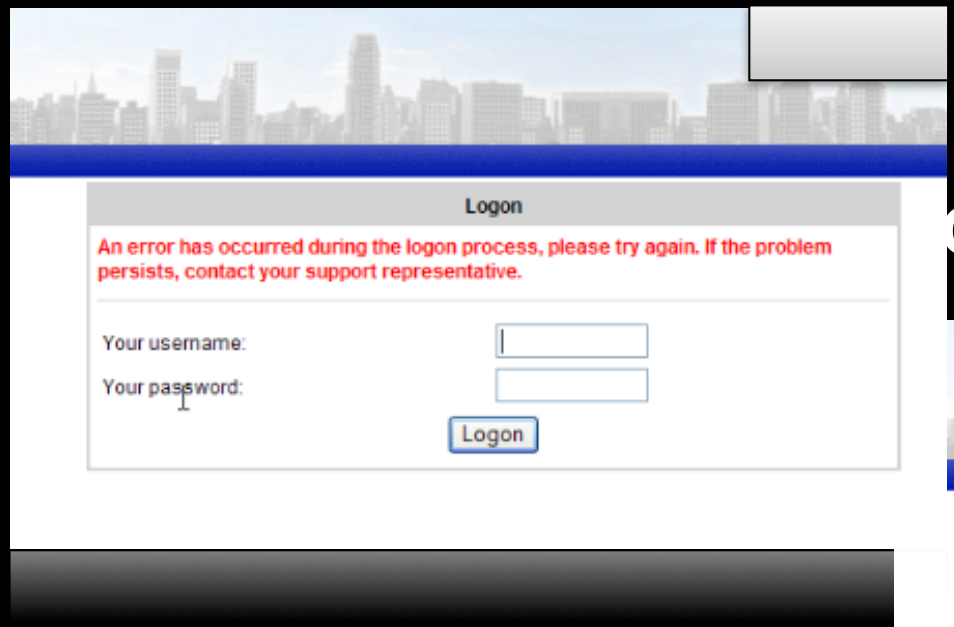
Don’t steal from these brands

```
entry "WebFilters"
   !http://*.webkinz.com/*
   !http://*.myspace.com/*
   !http://*.microsoft.com/*
   !http://*.skyblueads.com/*
```

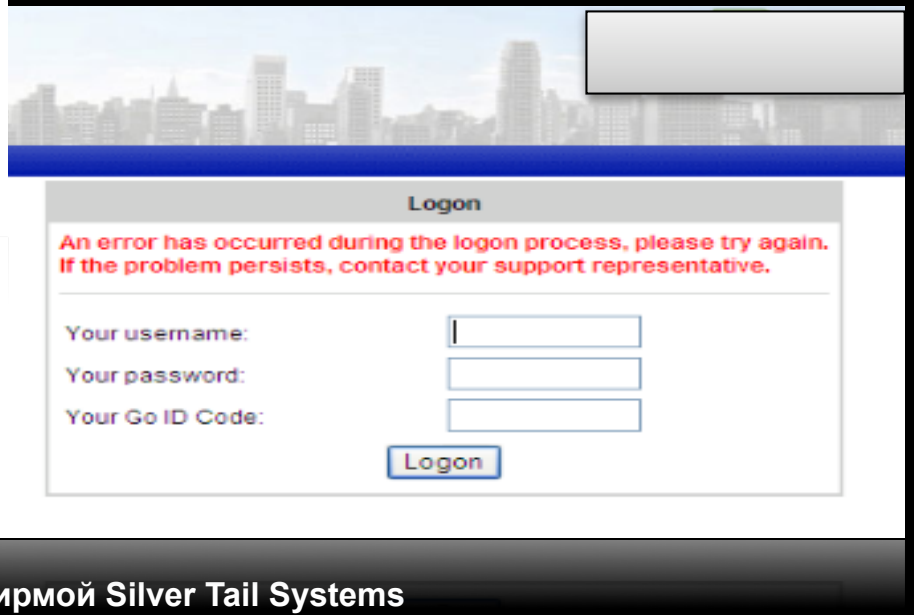
Материал предоставлен фирмой Silver Tail Systems

Внедрение элемента экрана

Обозреватель НЕ на узле Zeus:



Обозреватель на узле Zeus:



Материал предоставлен фирмой Silver Tail Systems

Статистика

- Трекер Zeus отслеживает 784 ботсети Zeus
- В ботсетях Zeus около 1,6 млн. ботов
- Атаки на 1130 брендов
- Около 960 – в финансовой сфере (85 %)
- КАЖДЫЙ из 5 крупнейших банков США атакуют свыше 500 ботсетей Zeus

Аналитический центр безопасности Cisco

Мощная поддержка средтсв безопасности Cisco

SensorBase

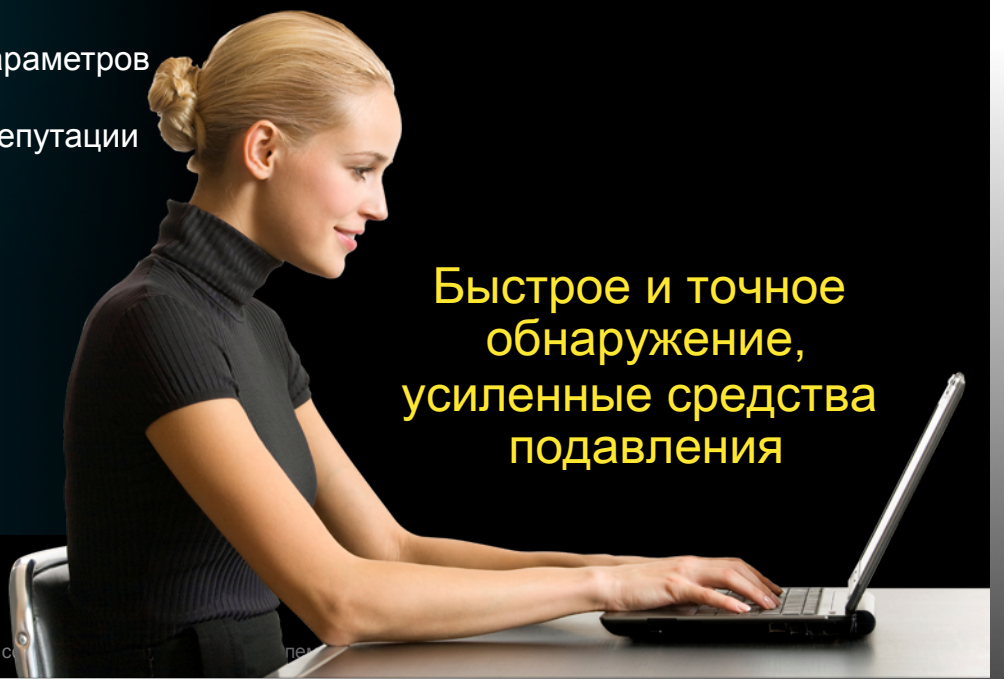
- В мире действует свыше 700 000 датчиков по четырем группам угроз
- Историческая библиотека 40 000 угроз
- 500 потоков информации от сторонних организаций, 100 потоков новостей, партнерства с разработчками ПО с открытым кодом и коммерческого ПО

Центр оценки угроз

- Автоматическое отслеживание более чем 200 параметров
- SenderBase: классифицирует и строит рейтинг репутации
- Корреляция угроз в мировых масштабах

Усиленная защита

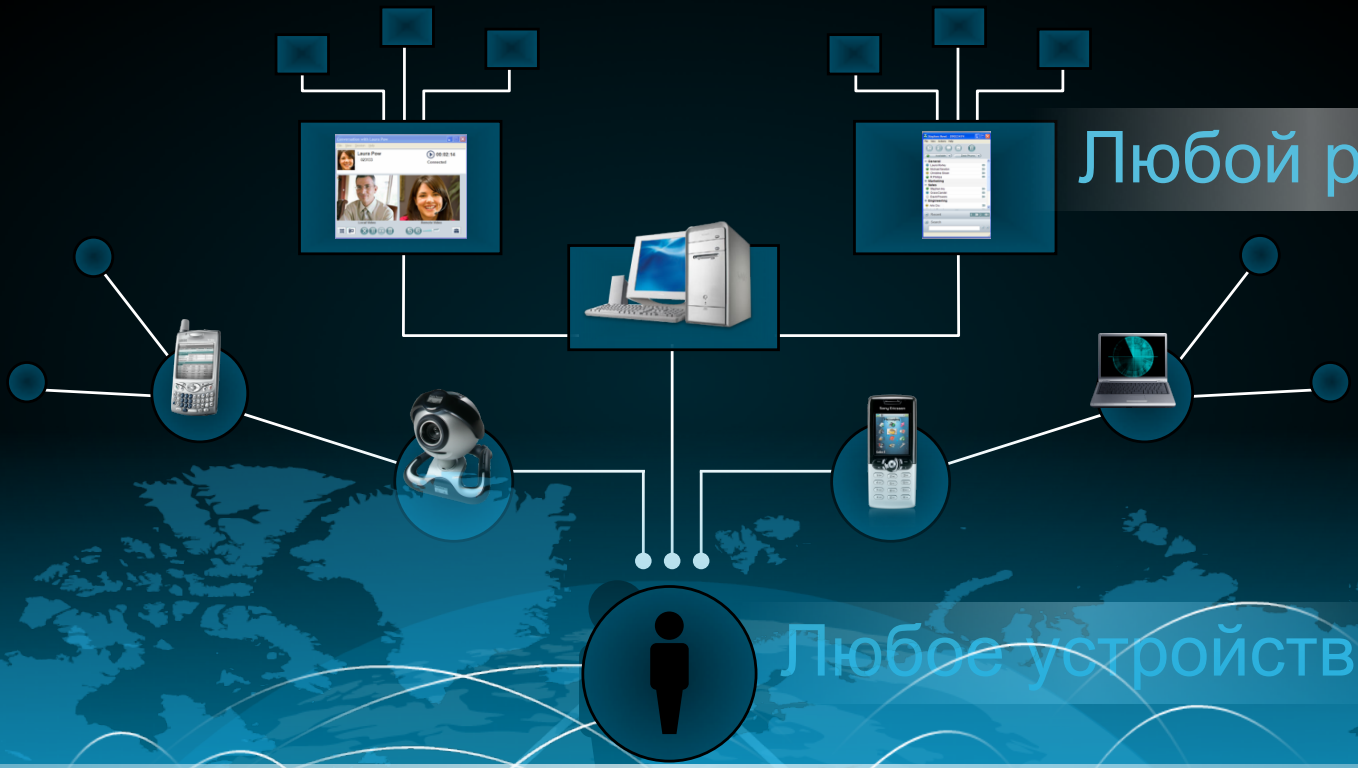
- Автоматическое создание правил и сигнатур
- Новейшие фильтры прорыва вируса



Быстрое и точное обнаружение, усиленные средства подавления

Подход Cisco к архитектуре

Преобразование:
Наше новое рабочее место – весь мир



СЕТИ БЕЗ ГРАНИЦ

Архитектура нового поколения как путь реализации нового рабочего пространства


CISCO