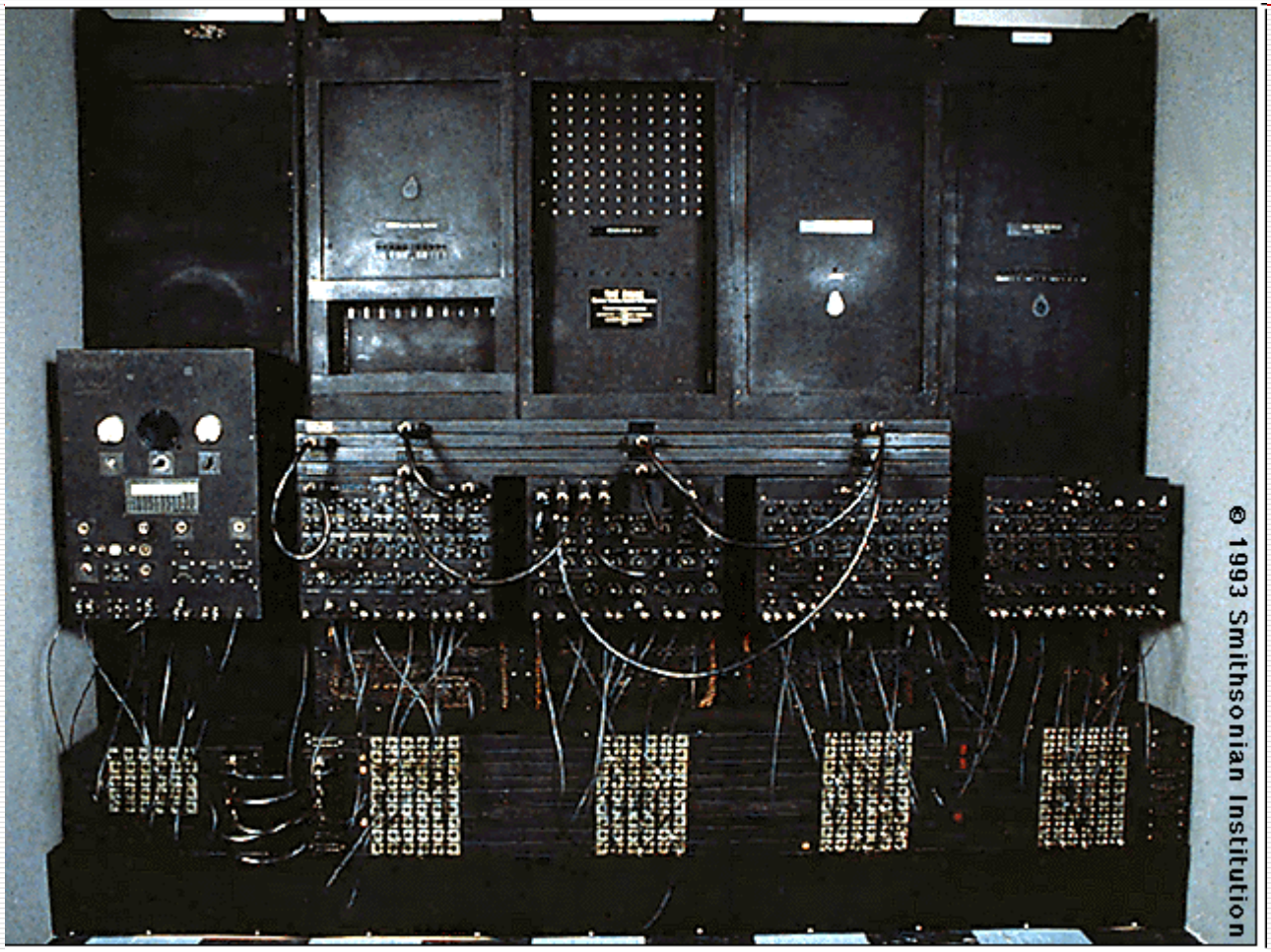
Привет, я - ENIAC



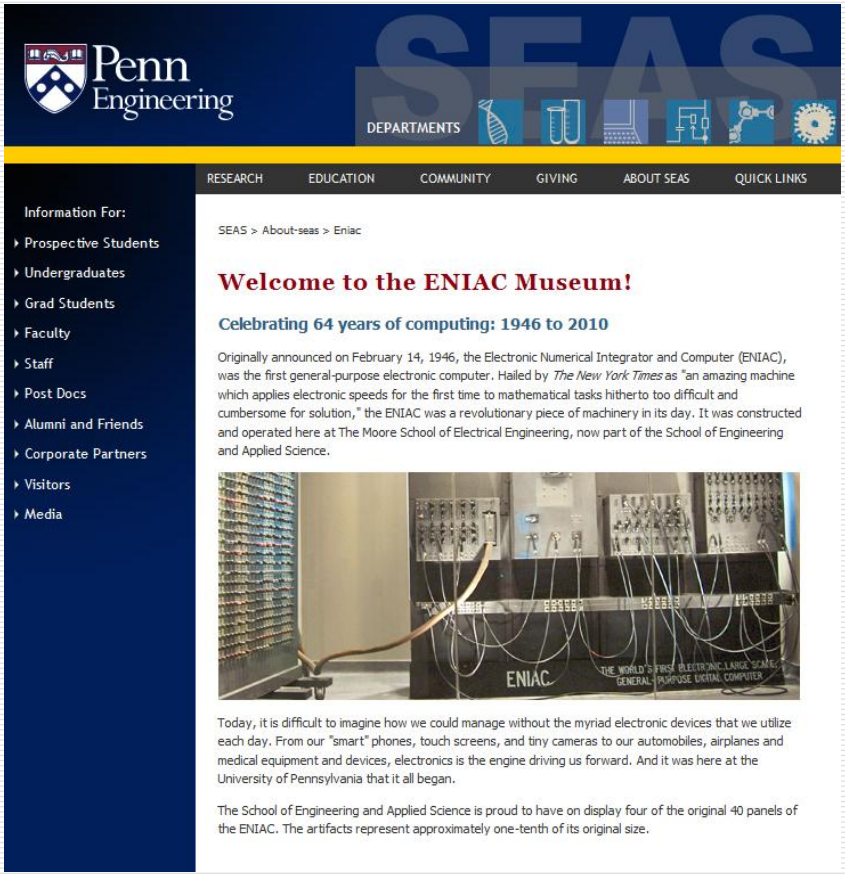
род. 1946 г.

А я – циано-бактериальный мат

род. ~3.5 млрд лет назад

Теперь нас можно встретить в...

- ...музее

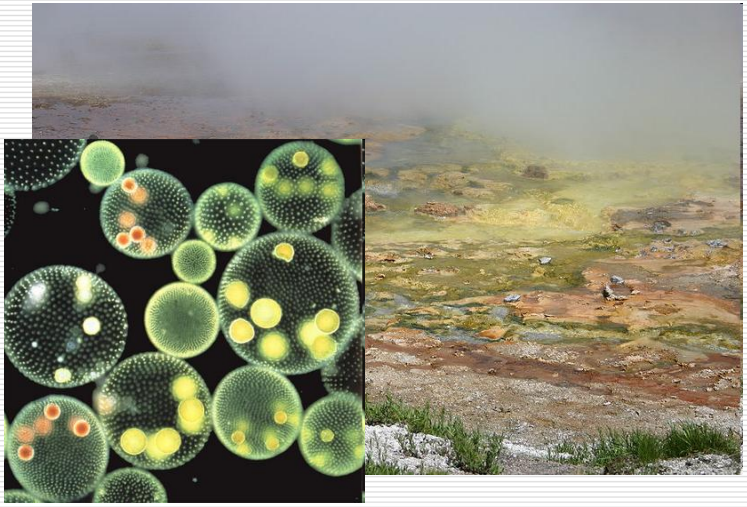


...И...

- ... заповеднике

Вытесненные более приспособленными

Шкала геологических эпох



3 млрд. лет

0,00000001 млрд. лет

Введение в информационную безопасность

Спецкурс кафедры АСВК ВМК МГУ

осенний семестр 2010 г.

Лекторы

- Денис Гамаюнов
  - м.н.с. ЛВК АСВК ВМК МГУ
  - соруководитель спецсеминара кафедры АСВК «Информационная безопасность и сети ЭВМ» с 2001 года
- Владимир Иванов
  - заместитель руководителя департамента эксплуатации «Яндекс»

Информационная поддержка курса

- Wiki: http://course.secsem.ru/
- Список рассылки: course@secsem.ru http://lists.secsem.ru/cgi-bin/mailman/listinfo/course

Программа курса

- Два семестровых спецкурса:
  - «Введение в информационную безопасность» - осенний семестр
  - «Практические аспекты безопасности компьютерных сетей» - весенний семестр
- Допуск к весеннему спецкурсу по итогам сдачи экзамена по осеннему спецкурсу

Программа осеннего семестра – 1/2

- **Введение**
  - Задачи информационной безопасности. Методы обеспечения информационной безопасности – криптография, модели безопасности, контроль поведения.
  - Программные уязвимости. Практические аспекты эксплуатации уязвимостей.
  - Инструменты. Статический и динамический анализ программ.
- **Основы криптографии и криптоанализа**
  - Шифрование. Хэширование. Криптоанализ. Простейший частотный анализ, атаки на криптографические протоколы.
  - Применение криптографии в сетях. SSL/TLS, ЭЦП, протоколы аутентификации, хранение credentials.
  - Протоколы PGP и S/MIME и их реализации.

Программа осеннего семестра – 2/2

- **Программные уязвимости – на стыке аппаратуры и программного обеспечения**
  - Язык ассемблера. Синтаксисы Intel и AT&T. Устройство процессора. Подпрограммы и функции. Передача аргументов, возврат значения. Системные вызовы. Размещение объектов в памяти.
  - Архитектура Linux. Загрузчик программных модулей. Формат исполняемых файлов ELF. Зависимости модулей. Символы. Утилиты objdump и ldd.
  - Уязвимости, связанные с переполнением буфера.
- **Механизмы защиты информации в современных операционных системах**
  - Формальные модели доступа. Дискреционные, мандатные модели. Модели Бела-ЛаПадулы, Биба. Ролевой доступ, RBAC, RSBAC.
  - Мандатный и ролевой доступ в Linux. GRSecurity, SELinux, RBAC в некоторых файловых системах. Настройка политик безопасности.

Немного теории

- Принято различать:
  - Конфиденциальность
  - Целостность
  - Доступность

Криптография?

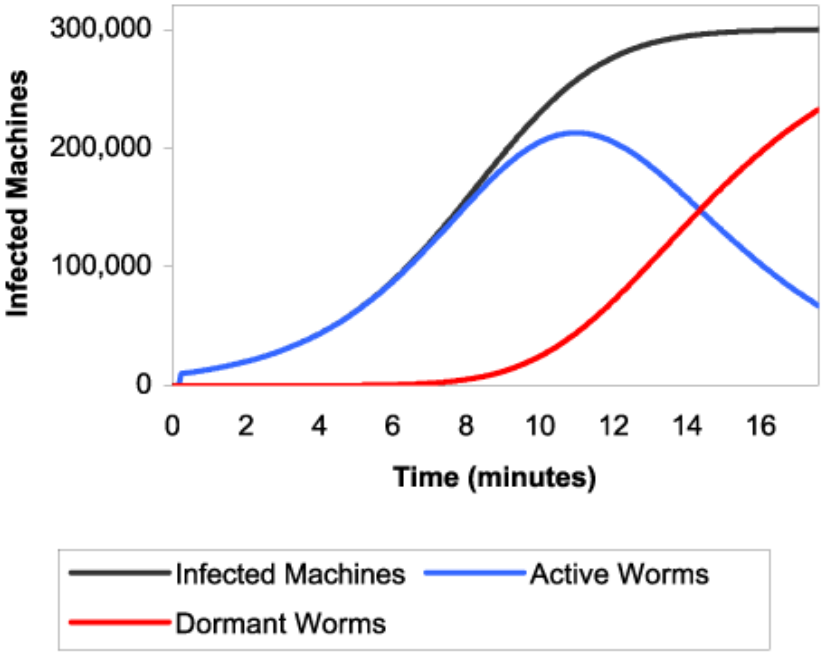
- Шифрование
  - Симметричные алгоритмы, хэширование, алгоритмы с открытыми ключами
  - SSL, VPN, тунеллирование
  - Авторизация и аутентификация
- Электронная подпись
  - Удостоверение подлинности
  - PEM, PGP
  - Проблема PKI (Public key infrastructure)

Не всегда и не везде

- Кража персональных данных (phishing)
- Мошенничество (scam)
- Вредоносное ПО
  - Вирусы
  - Трояны
  - Сетевые черви
- Массовые рекламные рассылки (spam)
- Организация DDoS-атак
- «Устойчивый к жалобам» веб-хостинг
- ...

Ботнеты – технологическая основа cybercrime

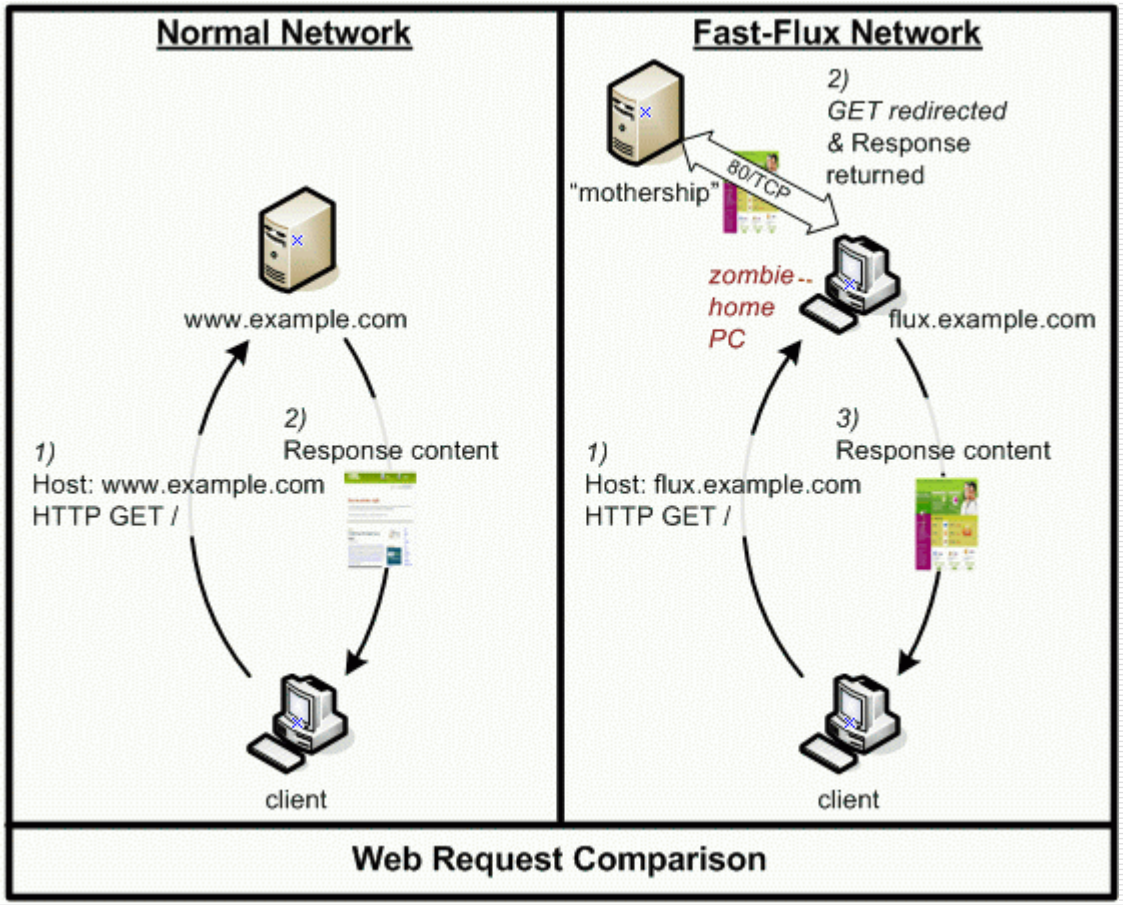
- Распространение через уязвимости в Adobe Flash, MS IE и т.д.
- Миллионы заражённых узлов
- Скрытность управления – Fast flux / double flux
- Разнообразие применения:
  - DDoS
  - Хостинг (malware, нелегальный контент и т.п.)
  - Money mules, scam, spam…



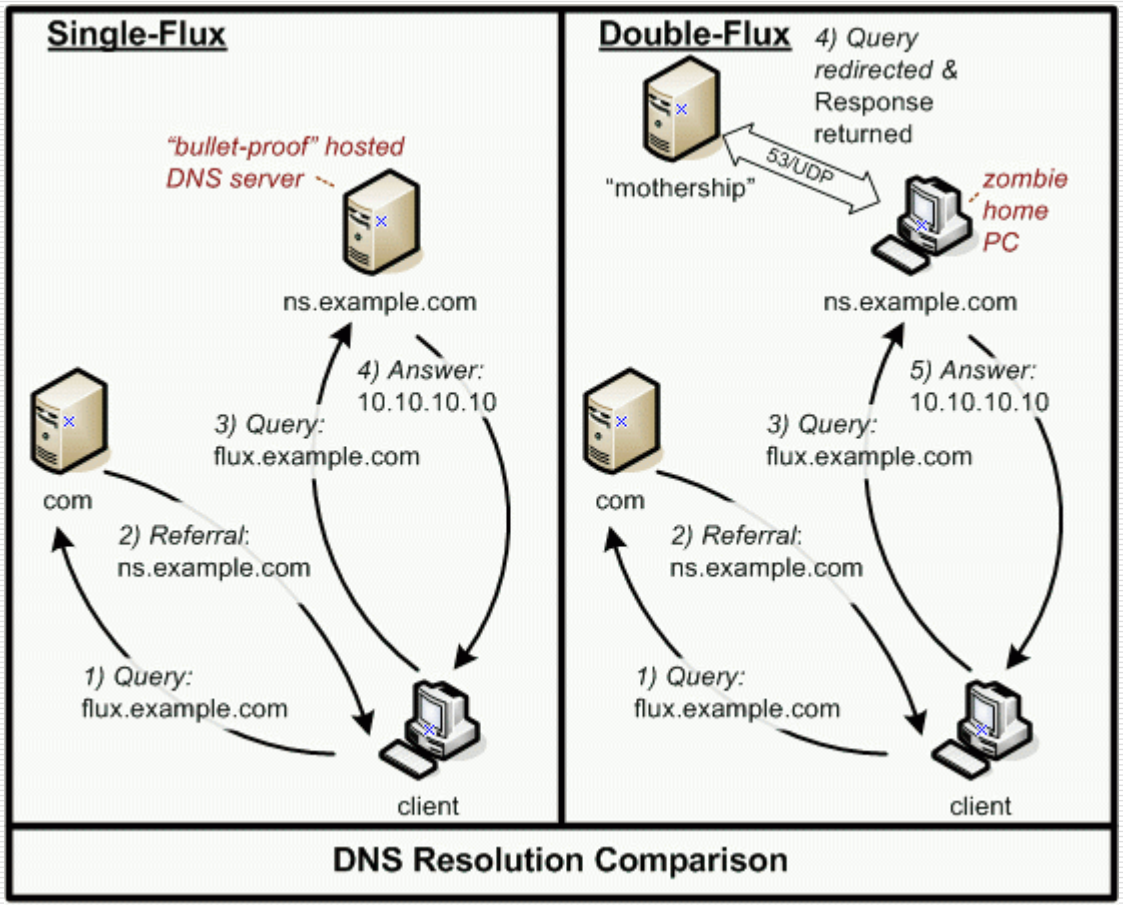
Fast-flux botnet: подробности

- «Контент» распределён по тысячам заражённых узлов в интернете.
- DNS-сервер домена (*www.example.com*) использует динамическую ротацию адресов в комбинации с очень коротким временем жизни записи (TTL) для каждой записи, за счет чего FQDN может иметь сотни или тысячи привязанных IP-адресов.
- Доменное имя может менять IP-адрес каждые 3 минуты.
- Соединяясь с одним и тем же доменом раз в 3 минуты, браузер, на самом деле, будет каждый раз соединяться с новым узлом.
- Адреса выбираются по интеллектуальной схеме, обеспечивая максимальную пропускную способность от клиента до сервера.

Fast-flux botnets: схема



Fast-flux botnets: double flux



Fast-flux: примеры

- Сети money-mule (divewithsharks.hk)
- Scam-сети (myspacee.com)
- Spam-сети (Warezov/Stration)
- Stormnet/RBN

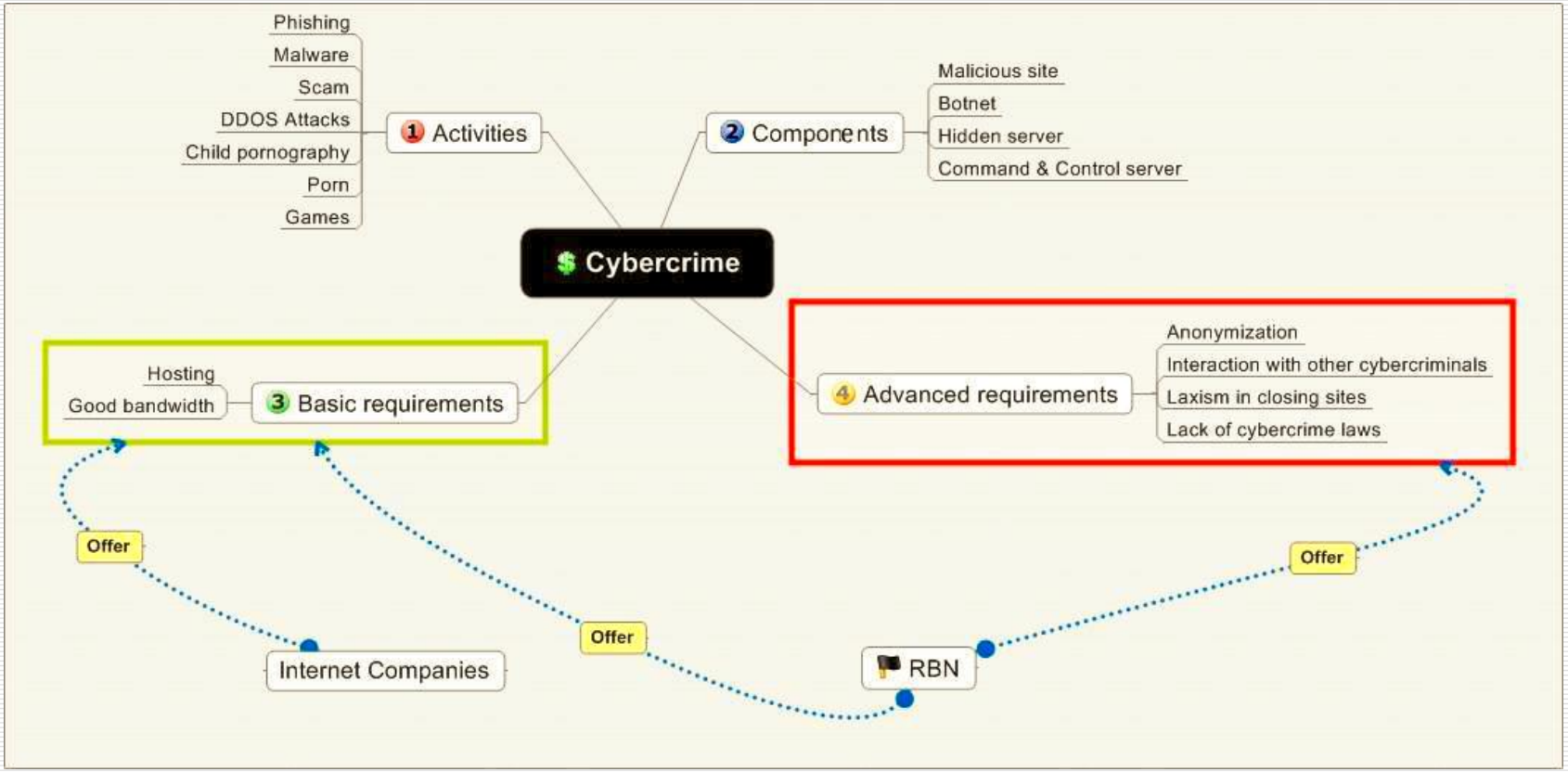
Stormnet

- Сентябрь 2007 г. – по различным оценкам, от 1 млн. до 50 млн. заражённых систем
- Разнообразие функций:
  - game0.exe - Backdoor/downloader
  - game1.exe – SMTP relay
  - game2.exe – кража e-mail адресов
  - game3.exe – распространение вирусов с помощью e-mail
  - game4.exe – средство организации DDoS-атак
- Коммуникационный протокол – eDonkey p2p
- Активность:
  - Сентябрь 2007 г. – компрометация сайта республиканской партии США, после чего с него идёт распространение
  - Октябрь 2007 г. – используя уязвимость в captcha Youtube.com, организуется рассылка целевой рекламы пользователям Xbox
  - Канун рождества 2007 г. – рассылка поздравительных открыток с троянами

Основные причины расцвета киберпреступности

- Недостатки стека TCP/IP
  - Анонимность трафика
  - Отсутствие контроля нагрузки в масштабах интернета
- Многочисленные программные уязвимости
  - Операционных систем
  - Прикладного ПО
- Человеческий фактор
  - Низкая техническая грамотность пользователей
  - Невнимательность и неосторожность

Russian Business Network (RBN)



RBN: распространение вредоносного ПО

- 2005 : CoolWebSearch – pop-up окна с рекламой
- 2006 : UrSnif – через уязвимость Vector Markup Language
- 2007: Mpack – встроенное в веб-страницу средство взлома. Способно заражать html-страницы и впоследствии взламывать клиентские узлы через уязвимости Windows, Internet Explorer, Winzip, Qucktime и т.д. Mpack встраивается в виде iframe в нормальные html-страницы. Кроме того, эти вставки перенаправляют пользователя на вредоносные сайты.
- 2007: взлом и заражение веб-сайта Банка Индии.
- 2007: Torpig/Sinoval – троян для сбора банковских данных пользователей. Как минимум в течение 3 месяцев со времени появления большинство антивирусов были не способны его выявлять.
- Активное распространение обычных троянов:
  - Rustock
  - Haxdoor
  - Pinch
  - прочие

RBN: phishing

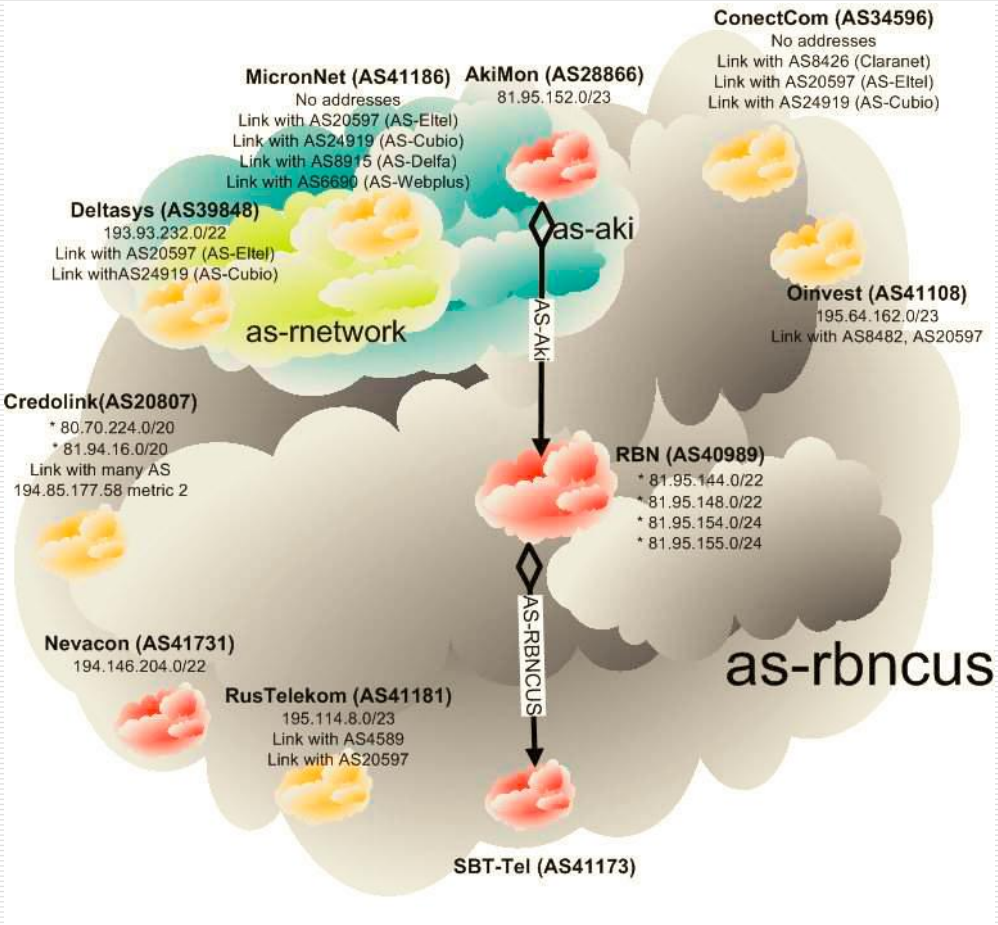
- Хостинг вредоносного ПО, используемого для фишинга
- Хостинг фишерских веб-сайтов

RBN: DDoS, спам и все-все-все

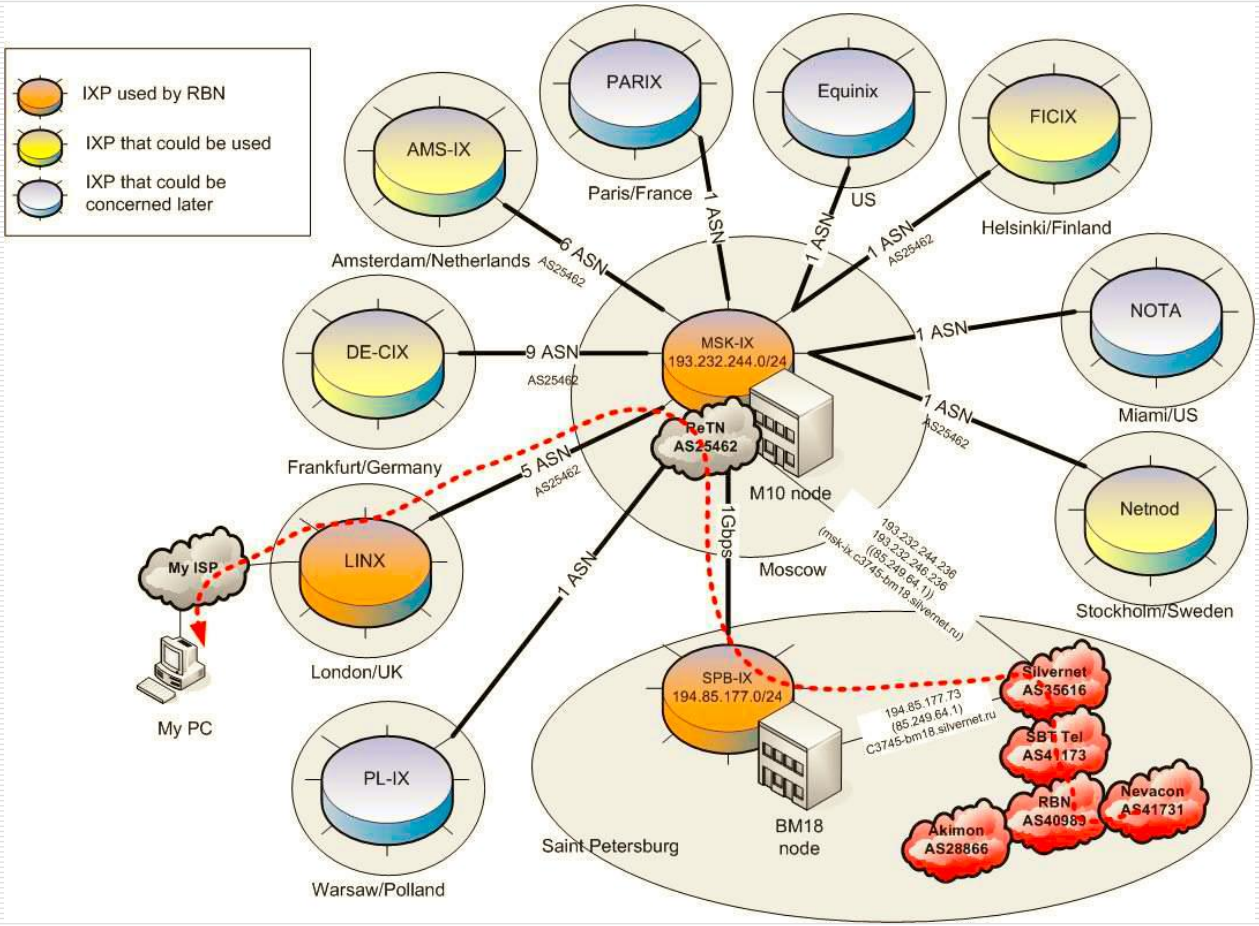
- SpamStock/Rustock – рассылка поддельных сообщений с финансовыми прогнозами, влияющие на биржи
- DDoS – атака на Банк Австралии в 2006 году в ответ на запуск новой системы защиты интернет-банка, после чего фишинговые схемы перестали работать
- Средства для автоматического взлома веб-сайтов
  - Icepack
  - Mpack
  - Webattacker

RBN: структура

- Автономные системы
- ISP
- IXP

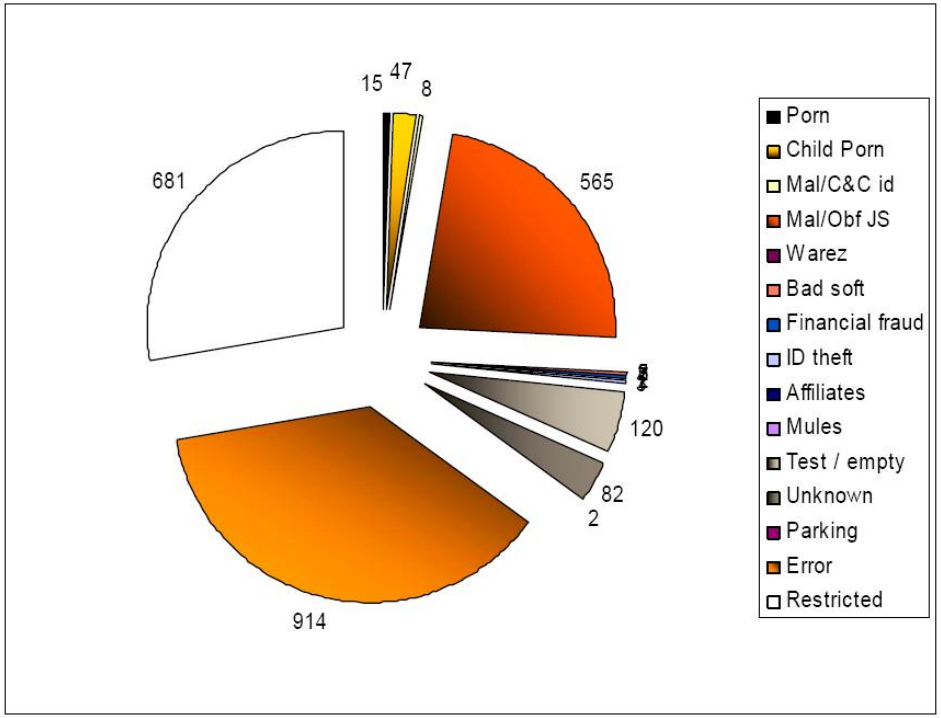


RBN: связи

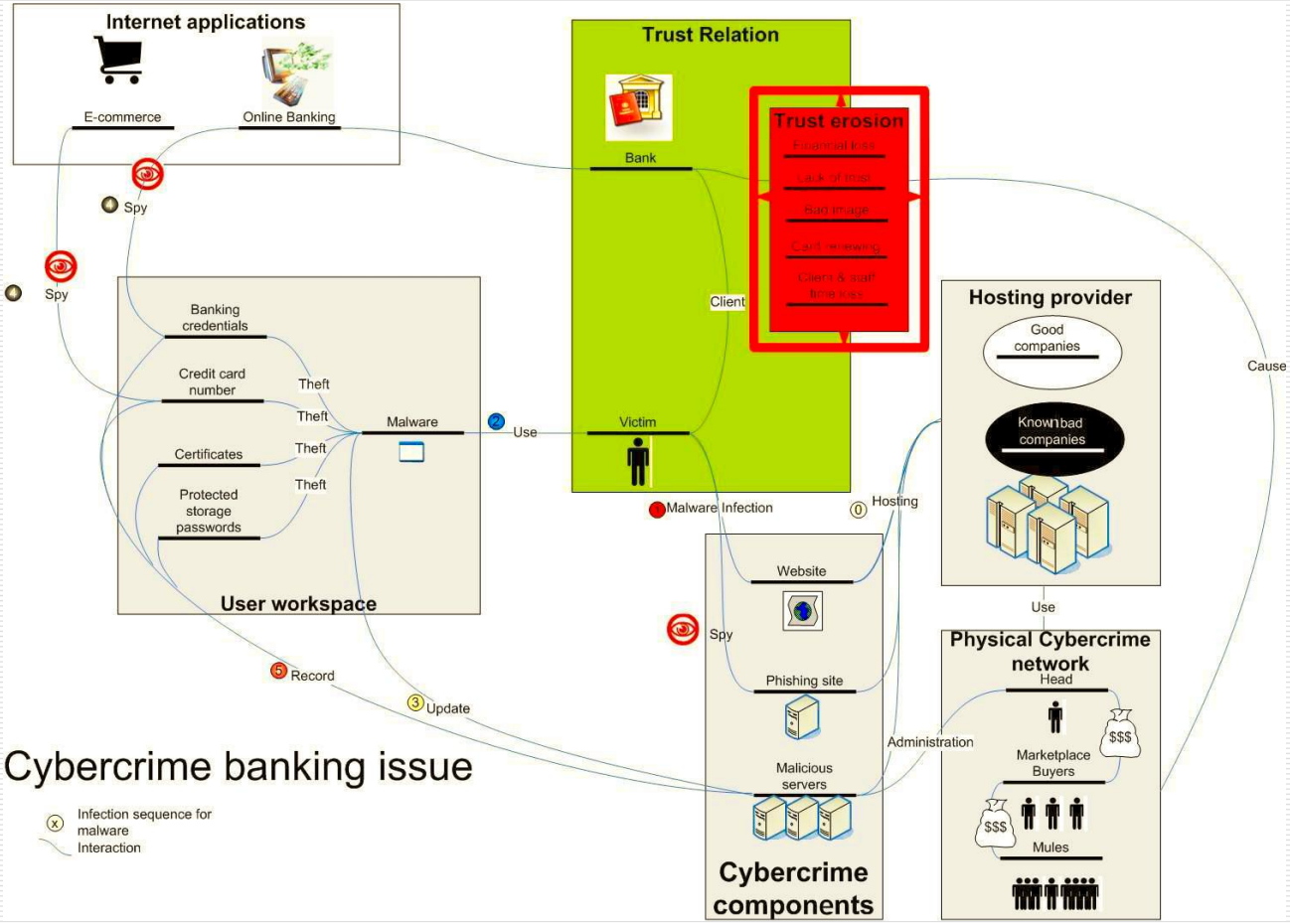

IXP used by RBN
IXP that could be used
IXP that could be concerned later
PARIX
Paris/France
Equinix
US
FICIX
Helsinki/Finland
AMS-IX
Amsterdam/Netherlands
NOTA
Miami/US
DE-CIX
Frankfurt/Germany
MSK-IX
193.232.244.0/24
ReTN
AS25462
M10 node
Moscow
Netnod
Stockholm/Sweden
LINX
London/UK
My ISP
My PC
PL-IX
Warsaw/Polland
SPB-IX
194.85.177.0/24
BM18
node
Saint Petersburg
Silvernet
AS35616
SBT Tel
AS41173
RBN
AS40989
Nevacon
AS41731
Akimon
AS28866
6 ASN
AS25462
1 ASN
1 ASN
1 ASN
AS25462
1 ASN
1 ASN
AS25462
9 ASN
AS25462
5 ASN
AS25462
1 ASN
1Gbps
193.232.244.236
193.232.245.236
((85.249.64.1))
(msk-ix.c3745-bm18.silvernet.ru)
194.85.177.73
(85.249.64.1)
C3745-bm18.silvernet.ru

RBN: клиенты

- 2090 доменов на 406 физических серверах
- Среди них ни одного «нормального» домена



RBN: структура активности



RBN: конец?

- В конце 2007 года сеть заблокирована
- Начало 2008: RBN “Rising”

Главное

- Многие из перечисленных проблем не могут быть решены одними лишь криптографическими методами