KASPERSKY lab

АКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ УГРОЗЫ

Александр Павлов

Руководитель группы подготовки и проведения тренингов

https://academy.kaspersky.ru/ ; https://securelist.ru/

ИСТОРИЯ ВРЕДОНОСНОГО ПО

Первые вирусные эпидемии (1981 - 1989): Brain (1986), червь Морриса (1988).

До-интернетовский период и интернет-этап (1990 - 2004): Chameleon (1990), Consept (1995), BackOrifice, Backdoor.BO (1998), Chernobyl (1998), LoveLetter (2000), Slammer (2003).

Современный криминальный этап (2005 – н.вр.)

ДИНАМИКА ПОЯВЛЕНИЯ НОВОГО ВРЕДОНОСНОГО ПО

1995 год: 1 вредоносная программа в час.

2005 год: 1 вредоносная программа в минуту.

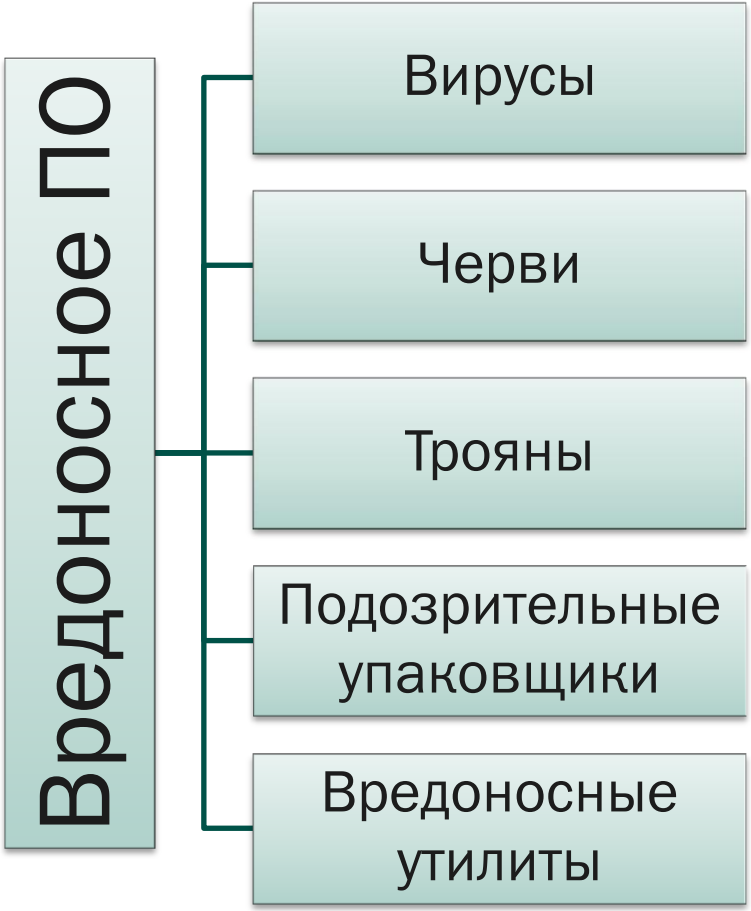
Н. вр.: 2 вредоносные программы в секунду.

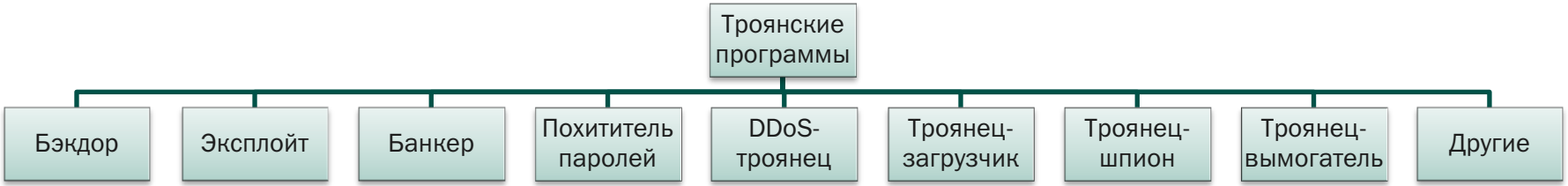
СОВРЕМЕННЫЕ ФИНАНСОВЫЕ ПОТЕРИ МИРОВОЙ ЭКОНОМИКИ ОТ КИБЕРУГРОЗ

Свыше 100 $млрд. в год

- Чистая прибыль Apple: 39,5 $млрд.
- Microsoft: 22 $млрд.
- IBM: 16,9 $млрд.
- Google: 14,4 $млрд.
- BMW: 2,7 млрд. евро
- Toshiba: 0,5 $млрд.
- Сбербанк: 392 млрд. руб.

ГЛОБАЛЬНЫЕ IT-УГРОЗЫ


Вредоносное ПО
Вирусы
Черви
Трояны
Подозрительные упаковщики
Вредоносные утилиты


Троянские программы
Бэкдор
Эксплойт
Банкер
Похититель паролей
DDoS-троянец
Троянец-загрузчик
Троянец-шпион
Троянец-вымогатель
Другие

ТЕХНИКА БЕЗОПАСНОСТИ

- Регулярное обновление ОС и ПО
- Антивирусное ПО
- Техника безопасности по отношению к вложенным файлам и ссылкам
- Регулярно делать бэк-апы
- Надежные пароли
- Техника безопасности в социальных сетях

Проверка надежности пароля:

https://blog.kaspersky.ru/password-check/

Пример. (Подбор пароля методом грубой силы).

- Предположим в пароле используются заглавные и строчные буквы латинского алфавита и цифры. Длина пароля – 8 символов. Компьютер проверяет 1 млн. вариантов в секунду.

- Всего 62 символа, количество вариантов:

$$62^8 \sim 64^8 = 2^{48} \sim 10^{15}$$

(учли, что $2^{10} \sim 10^3$). Таким образом, требуется 10^9 с. В сутках 86400 с. Всего требуется 11570 суток.

- Если злоумышленники используют ботнет из 100 тысяч компьютеров, то время для подбора пароля: $\sim 0{,}12$суток $= 3$ часа.

СОЦИАЛЬНЫЕ СЕТИ

Не публикуйте свою дату рождения, адрес, номер телефона, e-mail. Избегайте упоминания имен родственников и домашних животных, а также других данных, которые могут применяться в социально-инженерных атаках.

Дружить в социальных сетях только с людьми, которых вы хорошо знаете лично. Осмотрительно относится к содержанию постов, которые публикуются в режиме «для всех».

Отключить геотеги в фотографиях, которые вы публикуете. Не применять чекины (от англ.: check-in – отметки о географическом положении пользователя на карте) или создать очень маленький список тех друзей, для которых эти чекины будут доступны.

ЦЕЛЕВЫЕ АТАКИ

Целевые атаки	Классические атаки
Цель выбрана специально	Все является целью
Тихие и мгновенные атаки	Массивные и длительные вспышки заражений
Вредоносное ПО более совершенно	Вредоносное ПО менее совершенно и легче детектируется
Атаки остаются незамеченными длительное время	Атаки быстро обнаруживаются

АТАКА НА HBGARY FEDERAL (ФЕВРАЛЬ 2011)

Работает в области информационной безопасности. Заказчиком продукции является федеральное правительство США.

Февраль 2011 – генеральный директор HBGary заявил, что его компания знает, кто такие «Анонимусы».

Через несколько дней сайт компании был взломан (долгое время не обновлялся), был похищен список шифрованных паролей. Пароль CEO компании состоял из 8 символов. Этот же пароль использовался для доступа к корпоративной почте (на облачном сервисе Google для корпораций). Переписка компании с правительством попала в интернет.

КРАЖА СЕКРЕТОВ RSA

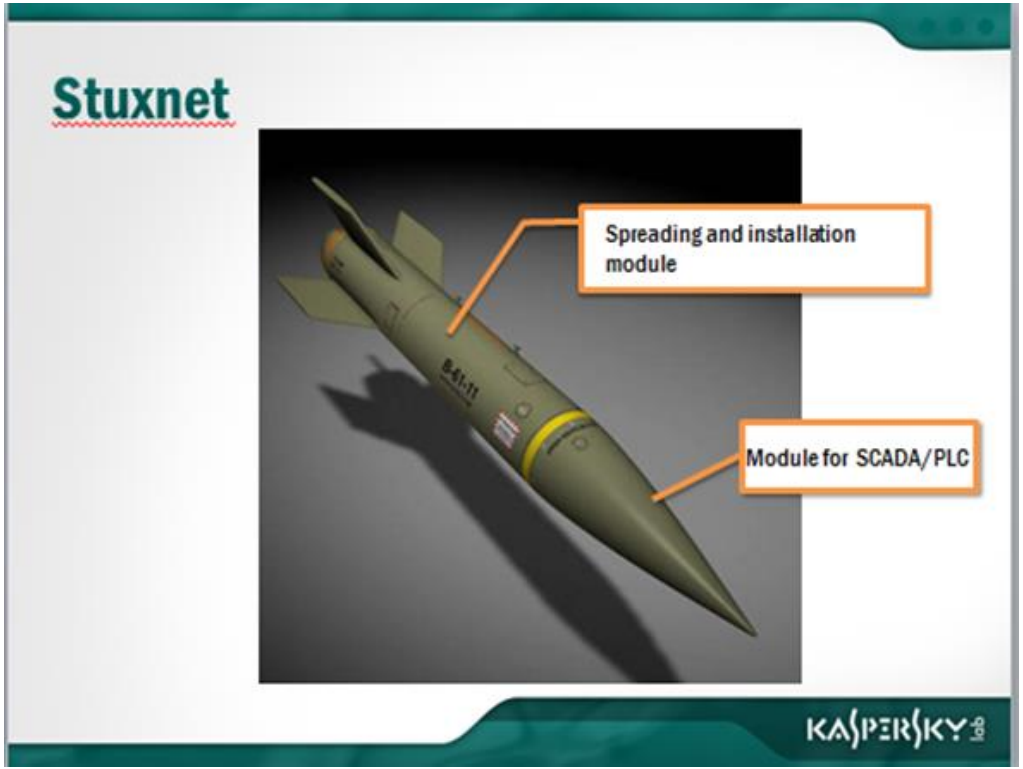
RSA (Rivest, Shamir, Adleman) - криптографический алгоритм с открытым ключом.

Спам-рассылка «План расширения кадрового состава в 2011 году» с вложенным в него зараженным xls-файлом.

В результате запуска эксплойта, внедренного в файл Excel, в систему был установлен «бэкдор».

Украденная информация: касалась средств многоуровневой аутентификации - технологии генераторов одноразовых паролей, карт персонального доступа к защищенным данным и пр.

СЕТЕВОЙ ЧЕРВЬ STUXNET (2010)



АТАКИ НА СИСТЕМЫ ОНЛАЙН-БАНКИНГА

РОССИЯ: ТОП-10 ИНТЕРНЕТ-БАНКОВ

Интернет-банк	% от аудитории интернета в России
Сбербанк России	40,2
Альфа-банк	8,2
ВТБ24	7,7
Русский Стандарт	4,3
ТКС Банк	3
Связной Банк	2,3
ХоумКредит Банк	2,2
Райффайзенбанк	2,2
Промсвязьбанк	1,7
Банк Уралсиб	1,5

ВИРУС-БАНКЕР ZEUS

Zeus – это троянская программа, появившаяся в 2007 году и предназначенная для атаки серверов и перехвата данных.
Zeus написан на Visual C++.

Распространение: среди прочего, программа использовала социальные сети (первый в истории пример такого рода вредоносного ПО). Через Facebook пользователям направлялись фотосообщения, которые переадресовывали на сайты с Zeus.

Количество атак, пришедшееся на модификации Zeus, выросло за 2013 год более чем вдвое, а число атакованных ими пользователей в данном году превысило показатели остальных банкеров из первой десятки вместе взятых.

CARBANAK

Целевая атака на банковский сектор.

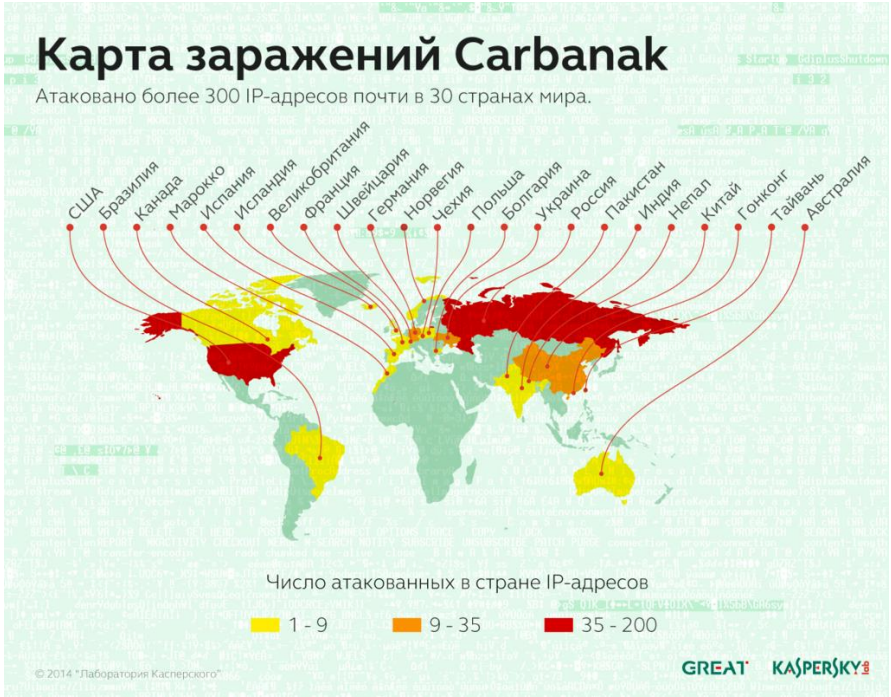
Пострадали десятки банков по всему миру.

Совокупный ущерб порядка 1 $млрд.

CARBANAK

KASPERSKY lab

CARBANAK



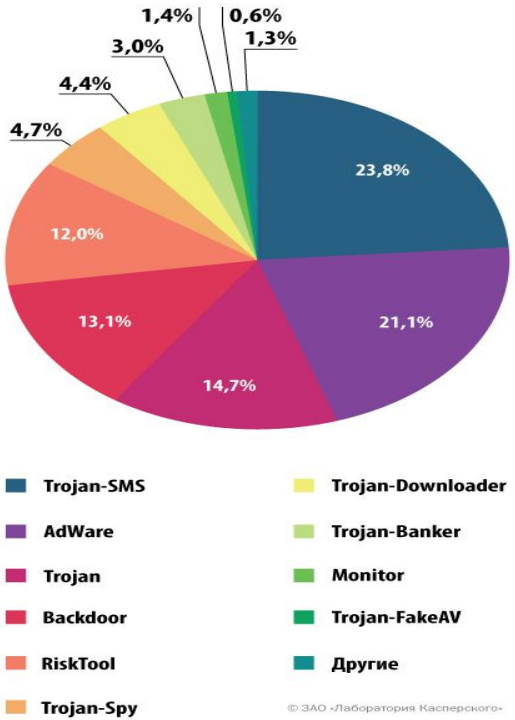
Первые образцы вредоносного ПО, используемого группировкой Carbanak, были созданы в августе 2013 года.

Первые заражения были обнаружены в декабре 2013 года.

Первые успешные кражи относятся к периоду с февраля по апрель 2014 года, пик числа заражений был зафиксирован в июне прошлого года.

МОБИЛЬНЫЕ УГРОЗЫ

СТАТИСТИКА ЗА 2014 ГОД



Распределение мобильных угроз по типам

4, 6 млн вредоносных установочных пакета;

300000 новых мобильных вредоносных программ;

12 000 мобильных банковских троянцев.

KASPERSKY lab

НОВЫЕ ТРЕНДЫ

Инфицирование легальных веб-ресурсов.

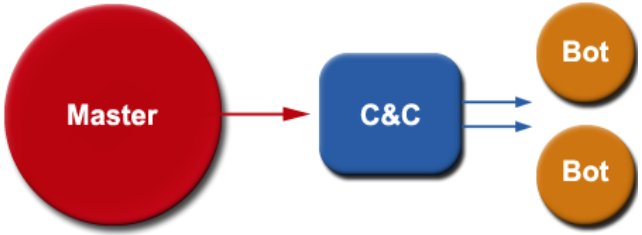
Распространение через альтернативные магазины приложений.

Эволюция и распространение вымогателей-блокировщиков.

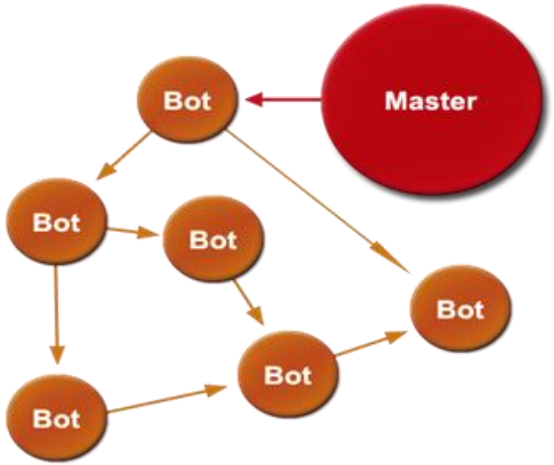
DDOS-АТАКИ

АРХИТЕКТУРА БОТНЕТОВ

Ботнеты с единым центром.



Децентрализованные ботнеты, или P2P-ботнеты.



ГРУППА РИСКА ДЛЯ DDOS-АТАК

- Самой излюбленной целью злоумышленников уже много лет является сегмент интернет-торговли (интернет-магазины, доски объявлений о продаже, аукционы и т.п.) - как правило, на эти сайты приходится большая часть всех зарегистрированных атак.

- На втором месте по популярности среди киберпреступников располагается финансовый сектор - различные бизнес-ресурсы, сайты банков, биржевые порталы.

- Третье место делят СМИ и ресурсы государственных организаций.

АТАКА НА АЭРОФЛОТ

Время атаки: 15-24 июля 2010 года.

Организатор атаки: генеральный директор компании ChronoPay Павел Врублевский. Исполнители: несколько человек под руководством ведущего специалиста по информационной безопасности компании ChronoPay.

Компьютерная атака блокировала работу системы оплаты электронных билетов на сайте "Аэрофлота". Это нанесло ущерб компании Assist на 15 миллионов рублей и более чем в 146 миллионов рублей оценивается ущерб "Аэрофлота".

СПАМ

E–mail: 2/3

Поставщики ПО, баз данных (электронных адресов), IP-адресов

Кроме того

- SMS
- IM
- Социальные сети

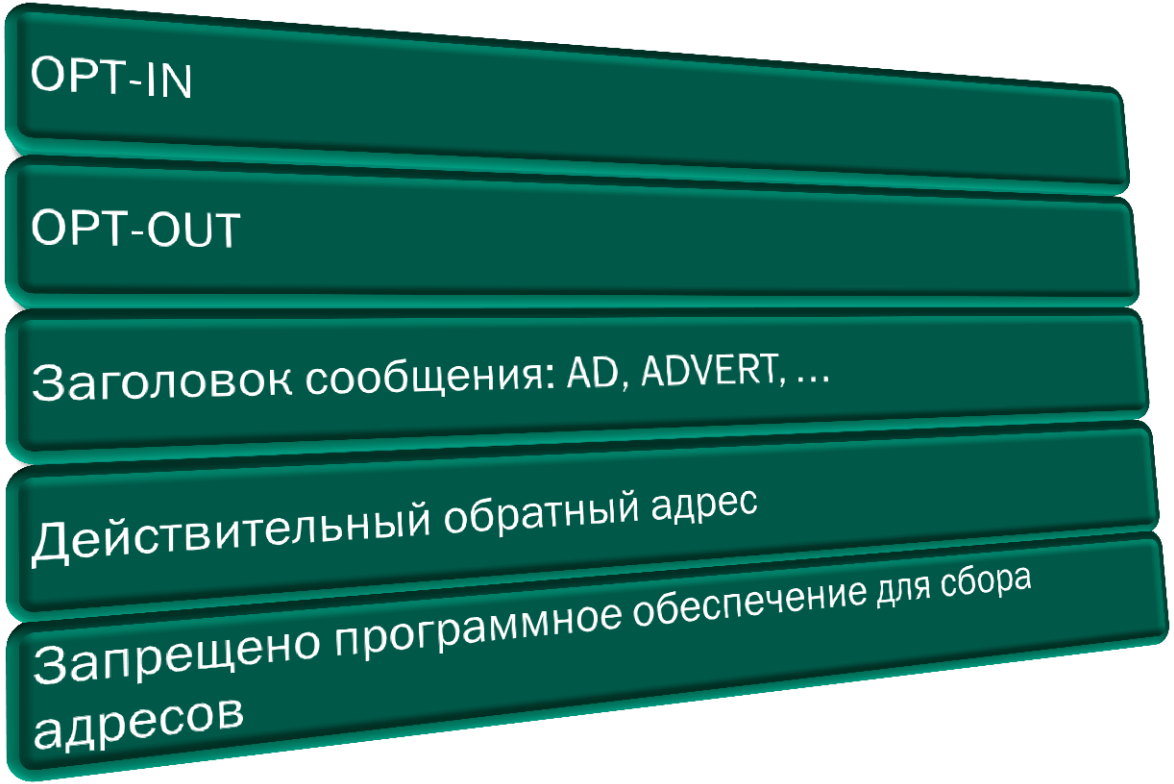
- Вирусописатели
- Сами спамеры (рассыльщики)
- Рекламодатели

РАСПРЕДЕЛЕНИЕ ИСТОЧНИКОВ СПАМА ПО СТРАНАМ

- 2008: Россия (22%), США (16%), Испания, Италия и Бразилия – на третьем месте с одинаковым показателем 5%.
- 2009: США (16%), Россия (8,5%), Бразилия (7,6%).
- 2010: США (11,3%), Индия (8,3%), Россия (6%).
- 2011: Индия (12,3%), Бразилия (7,5%), Индонезия (7%).
- 2012: Китай (19,5%), США (15,6%), Индия (9,7%).
- 2013: Китай (22,97%), США (17,63%), Южная Корея (12,67%).

- Нигерийские письма
- Цепочечные письма
- Фишинг
- Спам-письма с вредоносными вложениями

ЗАКОНОДАТЕЛЬНАЯ БОРЬБА СО СПАМОМ



САМООБУЧАЮЩИЕСЯ АНТИ-СПАМ АЛГОРИТМЫ

Формула Байеса

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{\sum_{j=1}^{n} P(A|B_j)P(B_j)}$$

$$P(S|A) = \frac{P(A|S)P(S)}{P(A|S)P(S) + P(A|H)P(H)}$$

S – ”Spam”

H – “Ham”

A – тестовое слово.

Случай k слов, которые входят в сообщение независимо:

Теорема.

$$P(S|A_1,\dots,A_k)=\frac{1}{1+\left(\frac{P(A_1)}{P(A_1|S)}-1\right)\dots\left(\frac{P(A_k)}{P(A_k|S)}-1\right)\left(\frac{1}{P(S)}-1\right)}$$

Доказательство.

$$P(S|A_1, \dots, A_k) = \frac{P(A_1, \dots, A_k|S)P(S)}{P(A_1, \dots, A_k)} =$$

$$\frac{P(A_1, \dots, A_k|S)P(S)}{P(A_1, \dots, A_k|S)P(S) + P(A_1, \dots, A_k|H)P(H)}$$

Так как

$$P(A_i|S) + P(A_i|H) = P(A_i)$$

и

$$P(A_1, \dots, A_k|S) = \prod_{i=1}^{k} P(A_i|S)$$

Получаем искомую формулу. Теорема доказана.

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab