лаборатория КАСПЕРСКОГО

Компьютерная преступность: причины и следствия

Евгений Касперский
руководитель антивирусных исследований
eugene@kaspersky.com

лаборатория КАСПЕРСКОГО

Кто и почему пишет вирусы. 198х-2005

- Тинейджеры, проба сил в программировании
- Компьютерные хулиганы
- “Исследователи” вирусных технологий. Вирусы класса Proof-of-Concept

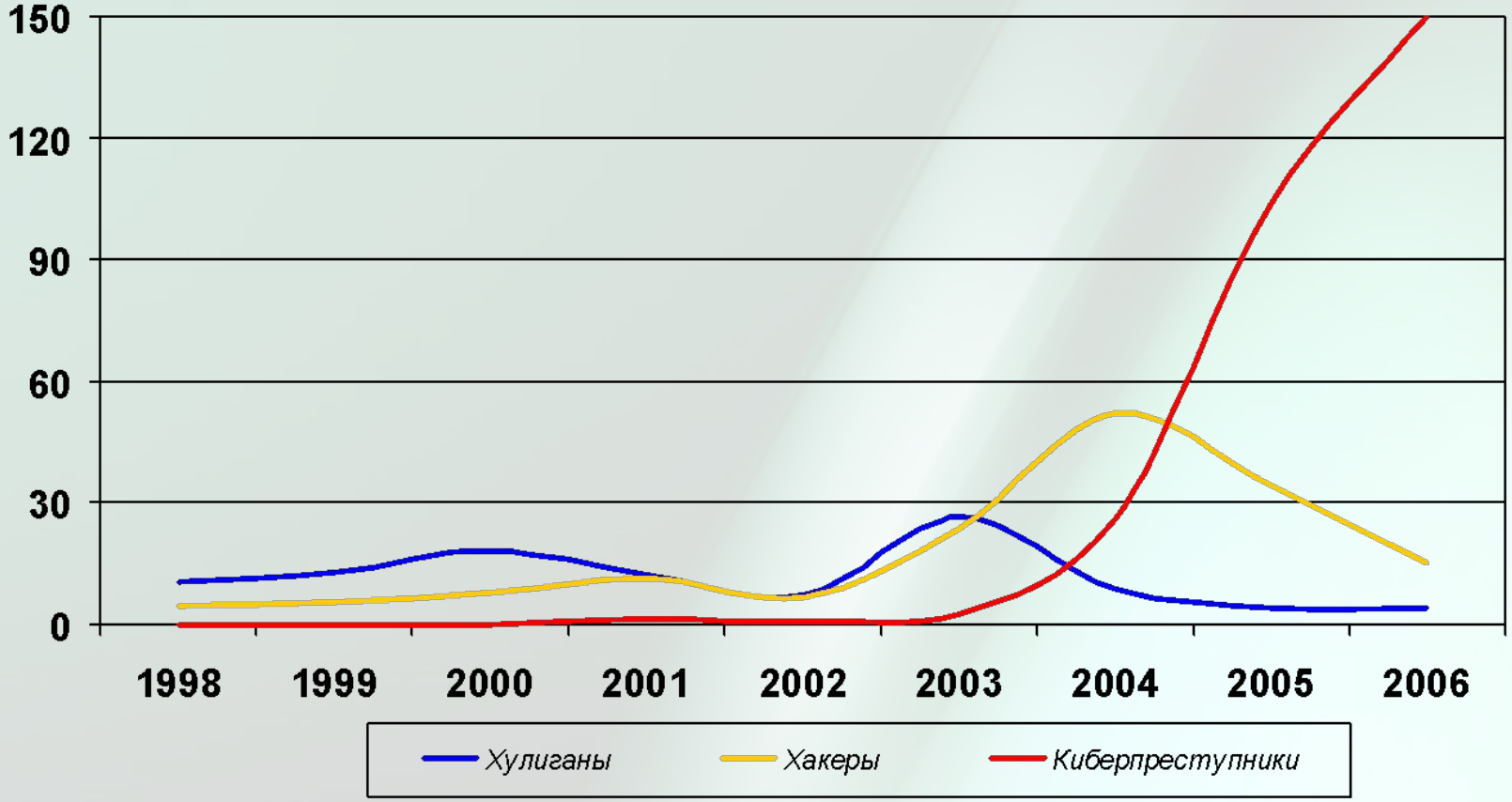
Кто и почему пишет вирусы. 198х-2005

Чен Инг Хау (Chen Ing-Hau), 24 года, Тайвань. Арестован 21 сентября 2000 за вирус “CIH”

Джефри Ли Парсон, 18 лет, США. Арестован 29 августа 2003 за вирус “Lovesan.b”

Свен Яшан (Sven Jaschan), 18 лет, Германия. Арестован 7 мая 2004 за серию вирусов “NetSky” и “Sasser”

Вирусная индустрия быстро криминализуется



Source: Kaspersky Lab

Кто и почему пишет вирусы и троянские программы

Традиционные вирусы – всё меньше и меньше…

Причины:

- Миграция в криминальный бизнес
- Громкие аресты вирусописателей в 1999-2004 гг.
- Развитие многопользовательских онлайн-игр

лаборатория КАСПЕРСКОГО

Кто и почему пишет вирусы и троянские программы

Эволюция целей и методов создателей вредоносных программ

1998

- мелкое воровство информации. AOL PSW Trojans
- троянские системы удалённого администрирования

2000-2001

- системы принудительного показа рекламы (AdWare)

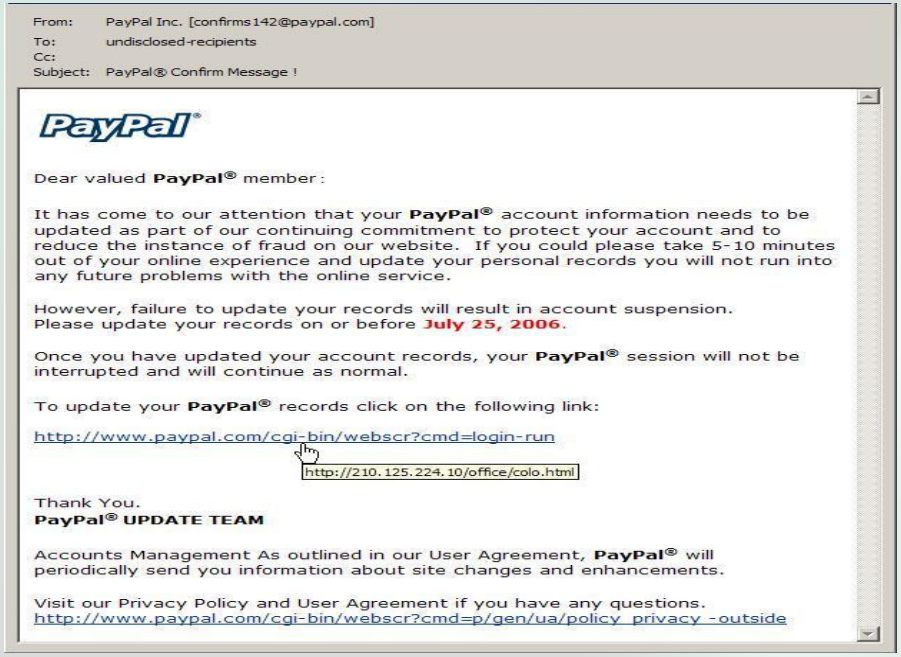
2002

- воровство электронных кошельков (Webmoney, e-Gold)
- троянские “звонилки” (Dialers) на платные номера

Кто и почему пишет вирусы и троянские программы

2003

- воровство персональных банковских кодов фишинг (поддельные банковские рассылки)
- сети троянских “proxy”-серверов для рассылки спама



From: PayPal Inc. [confirms142@paypal.com]
To: undisclosed-recipients
Cc:
Subject: PayPal® Confirm Message !

PayPal®

Dear valued **PayPal®** member :

It has come to our attention that your **PayPal®** account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension.
Please update your records on or before **July 25, 2006**.

Once you have updated your account records, your **PayPal®** session will not be interrupted and will continue as normal.

To update your **PayPal®** records click on the following link:

http://www.paypal.com/cgi-bin/webscr?cmd=login-run

http://210.125.224.10/office/colo.html

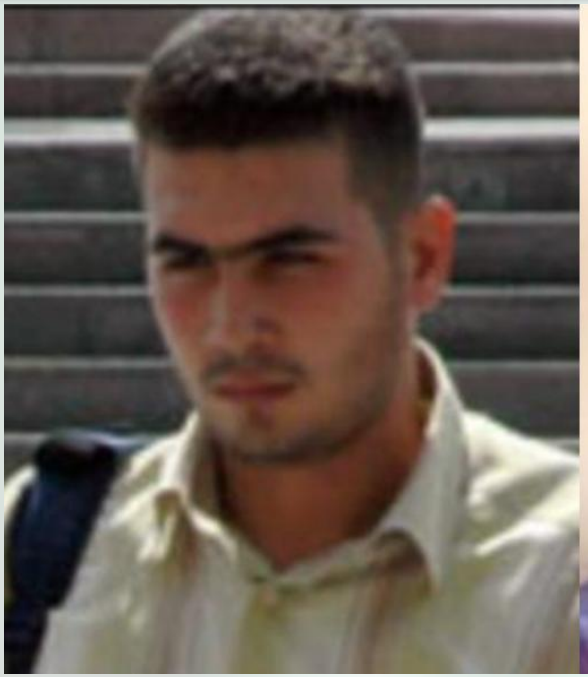
Thank You.
PayPal® UPDATE TEAM

Accounts Management As outlined in our User Agreement, **PayPal®** will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside

Кто и почему пишет вирусы и троянские программы

Джеймс Анчета (Jeanson James Ancheta), 20 лет, США. Арестован 3 ноября 2005 за создание “зомби-сетей” и сдачу их в аренду для рассылки спама и DDoS-атак на Web-сайты



Фарид Эссебар (Farid Essebar), 18 лет, Марокко и Атилла Экичи (Atilla Ekici), 21 год, Турция. Арестованы 26 августа 2005 за создание “зомби-сетей” при помощи червей “Mytob” и “Zotob” (“Bozori”)

Кто и почему пишет вирусы и троянские программы

2004

- ложные анти-шпионские (Anti-SpyWare) или антивирусные утилиты
- DDoS-атаки, рэкет, вымогательство

В настоящее время наблюдается заметное уменьшение количества DDoS-атак, причинами которого стали:

- Технические средства защиты
- Аресты злоумышленников в момент передачи выкупа

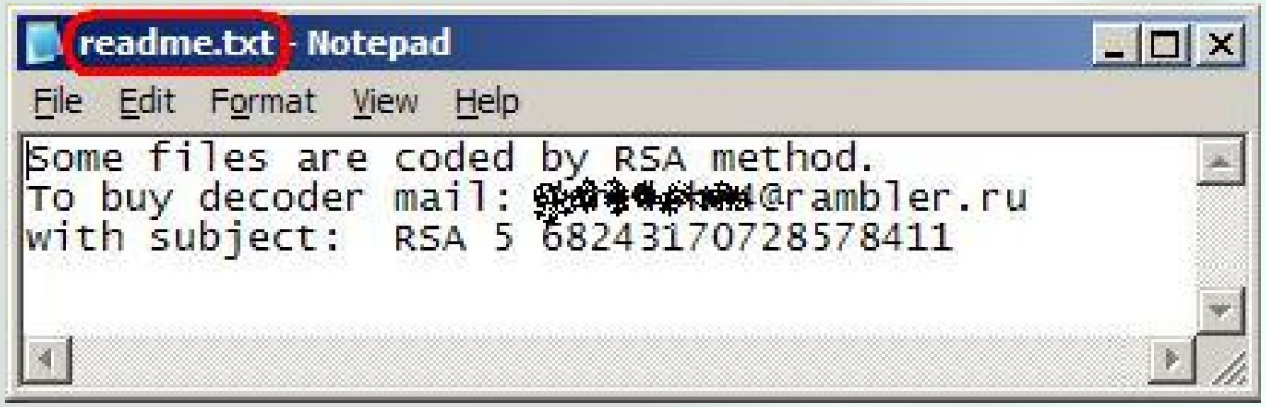
Кто и почему пишет вирусы и троянские программы

Россия, осень 2003 – весна 2004гг. DDoS-атака на британские онлайновые букмекерские конторы с последующим требованием денег за прекращение атаки. 20 и 21 июля 2004 года за проведение атаки в Санкт-Петербурге, Саратове и Пятигорске произведены аресты девяти человек. Организаторы атаки Мария Зарубина и Тимур Арутчев объявлены в розыск. Трое хакеров из их группы были приговорены к восьми годам колонии строгого режима в октябре 2006

Кто и почему пишет вирусы и троянские программы

2005

- воровство (сбор) электронных адресов для продажи спамерам
- поиск и продажа уязвимостей в ОС и приложениях
- “захват” информации с требованием выкупа (кибер-шантаж)
- “точечные” атаки на критически важные ресурсы



Сообщение о зашифрованных файлах и требование выкупа, которое оставляла троянская программа “GpCode”.

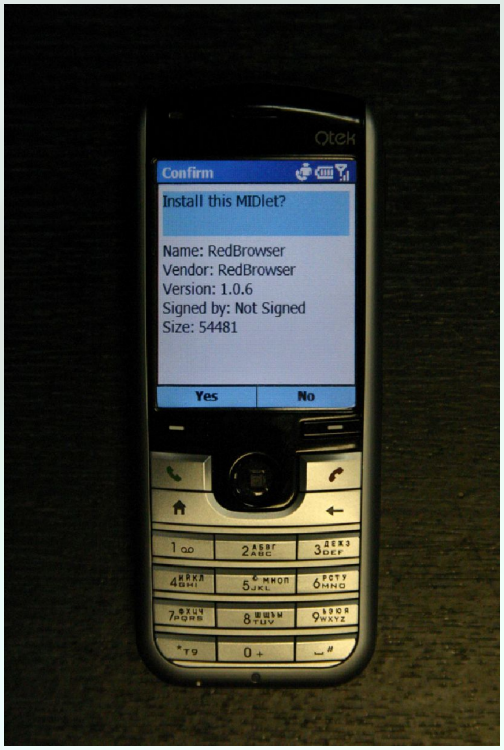
Кто и почему пишет вирусы и троянские программы

Ярон Болонди (Yaron Bolondi), 32 года, Израиль. Арестован 16 марта 2005 за взлом сети Лондонского отделения банка Сумитомо и попытку перевода со счетов банка 220 млн. фунтов стерлингов (более 420 млн. долларов США)

Кто и почему пишет вирусы и троянские программы

2006

- рассылка SMS на платные номера
- сопутствующий бизнес: анти-антивирусные технологии



Смартфон, зараженный троянской программой “RedBrowser”. Троянец рассылает SMS на платный номер

Кто и почему пишет вирусы и троянские программы

corpsespyware.net - Nuclear Grabber - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://corpsespyware.net/nuclear.htm

аналогичных "ID Lock" от ZoneAlarm

Несомненным плюсом является так же то, что логи отсылаются мгновенно - параллельно с данными, отсылаемыми на оригинальный сайт. Не нужно беспокоится о том, что холдер уйдёт в оффлайн и накопленный локально лог формграббера не успеет отослаться.

- WM-grabber тянет ключи, WMID, pass ; поддержиывает enum-авторизацию и железозависимый формат ключей
  Теперь поддержка и НОВОЙ версии WMKeeper 3.0 !
- Screenshot'ы по указанным адресам - позволят получать снимки экрана юзера и видеть то, что невозможно получить другими способами.
- собирает пароли Protected Storage (IE autocomplete, protected sites, outlook)
- собирает пароли почтового клиента TheBat!
- обходит файерволы
- блкирует обновление антивирусов (без hosts файла!)
- shell доступ с возможностью бэкконнэкта
- выполнение комманд всей армией сразу или конкретным ботом
- socks 5 сервер
- не виден в списке процессов во всех версиях windows 98/ME/2k/2k3/XP(SP1,SP2), файлы не видны на диске, у файлов системная дата идентична основным системным библиотекам
- записи в реестре защищены от удаления
- реализация без использования COM
- поддерживает 98/ME/2k/XP.
- написано на чистом ASSEMBLERe. размер 21кб

- что самое главное - всё вышеуказанное проверенно в реальных "боевых" условиях и наглядно продемонстрировало уязвимости в финансовых учреждениях по всему миру

- Для работы необходим любой хостинг с поддержкой PHP. Нет необходимости указывать пароль и логин к ftp в трое, а значит данные будут не только быстро получены, но надёжно сохранены.
- Существует возможность указывать резервные адреса, куда будут отсылаться логи, если основной вдруг станет недоступен.

цена *3000 USD* скидки постоянным клиентам. мы всегда готовы к конструктивному диалогу!

*** у нас широкий ценовой диапазон и при желании можно подобрать альтернативное spyware, которое будет максимально подходить под ваши потребности и возможности
***

оплата принимается через WebMoney (http://www.webmoney.ru) и e-gold (http://egold.com)
зачисление другими е-валютами по договорённости
другие формы оплаты - по договорённости (наличие технической возможности и лохов, которые будут эту возможность обеспечивать)

ПО ВОПРОСАМ ПРИОБРЕТЕНИЯ ТОЛЬКО ICQ #670045

Объявление о продаже вредоносной программы, способной блокировать работу антивирусов

Критически опасные технологии

1. Шифрование пользовательской информации кодом с высокой степенью защиты

Примеры вредоносных программ:

- **Cryzip (США)**

Проводит архивирование пользовательских файлов (с удалением оригинала файла) под паролем. Используется сложный пароль большой длины

- **GPCode (Россия, Украина?)**

Алгоритм RSA, ключи длиной 56, 64, 260, 330, 660 бит (на подбор ключа потребовалось бы 30 лет работы одного компьютера с тактовой частотой 2,2 GHz)

При использовании подобных или более стойких методов шифрования восстановить данные без помощи злоумышленника невозможно!

лаборатория КАСПЕРСКОГО

Критически опасные технологии

1. Шифрование пользовательской информации кодом с высокой степенью защиты

```
OUR E-GOLD ACCOUNT: 2934487

INSTRUCTIONS HOW TO GET YUOR FILES BACK
READ CAREFULLY. IF YOU DO NOT UNDERSTAND, READ AGAIN.

This is automated report generated by auto archiving software.

Your computer catched our software while browsing illigal porn
pages, all your documents, text files, databases was archived
with long enought password.

You can not guess the password for your archived files - password
lenght is more then 10 symbols that makes all password recovery
programs fail to bruteforce it (guess password by trying all
possible combinations).

Do not try to search for a program what encrypted your information - it
is simply do not exists in your hard disk anymore.
If you really care about documents and information in encrypted files
you can pay using electonic currency $300.
Reporting to police about a case will not help you, they do not know
password. Reporting somewhere about our e-gold account will not help
you to restore files. This is your only way to get yours files back.
```

Требование выкупа от троянской программы “Cryzip”

Критически опасные технологии

2. Противодействие антивирусным технологиям

- **Атаки на продукты:**
  - остановка продукта или апдейтера
  - изменение настроек продукта
  - авто-нажимание на клавишу “Skip”
  - руткиты (средства, скрывающие присутствие вредоносных программ)

лаборатория КАСПЕРСКОГО

Критически опасные технологии

2. Противодействие антивирусным технологиям

- **Атаки на технологии:**
  - обход эвристических сканеров
  - шифровка и/или паковка исполняемых файлов-троянцев
  - мутация кода в различных троянцах, иногда – каждого экземпляра троянца

Критически опасные технологии

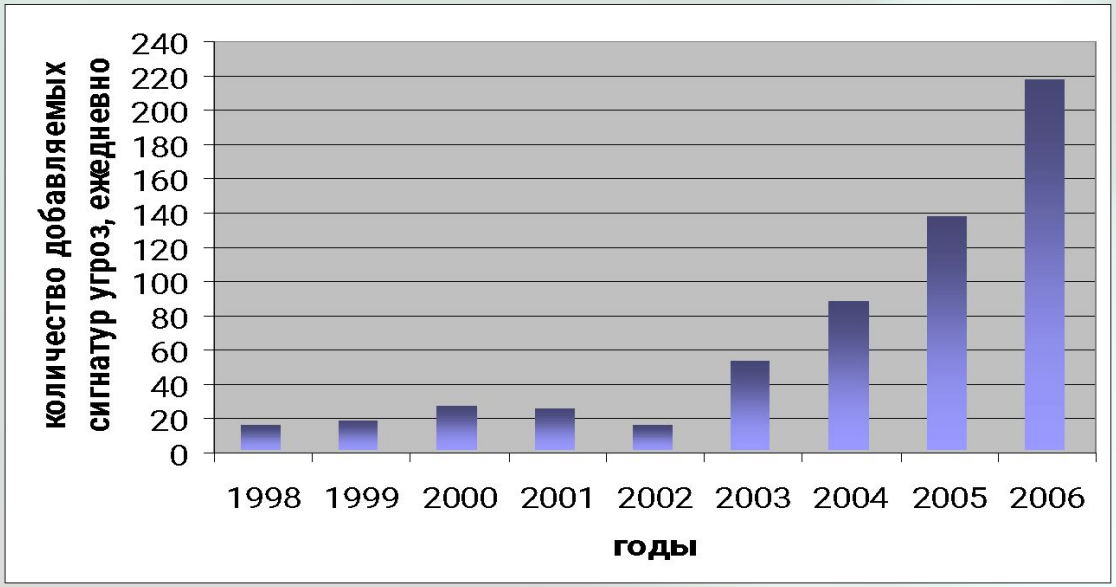
2. Противодействие антивирусным технологиям

- **Атаки на вирусные лаборатории:**
  - генерация многочисленных троянцев за короткий промежуток времени
  - подмена файла на заражённом сайте, если запрос на скачивание подается с IP-адреса антивирусной компании

Ситуация обостряется

1. Количество добавляемых записей растёт лавинообразно
2. Вредоносные программы становятся многочисленней и технологичнее

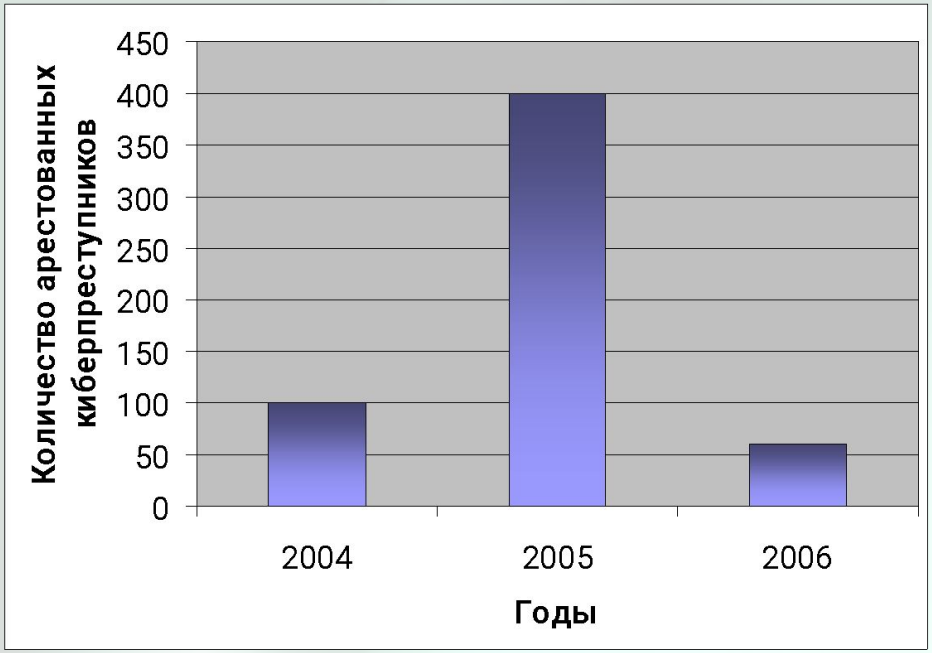
Вывод: если ситуация не изменится, то скоро разработчики антивирусных программ не смогут обеспечивать адекватную защиту



Изменение количества ежедневно добавляемых сигнатур угроз

На той стороне баррикад

1. Численность киберпреступников быстро увеличивается
2. Появляются новые киберпреступники, а старых не становится меньше



Вывод: Существующие методы полицейских расследований не работают против современных преступников

На той стороне баррикад

Опыт взаимодействия с полициями нескольких стран показывает, что расследования киберпреступлений в большинстве случаев проходят успешно

1. **Увеличение инвестиций в полицейские расследования**
2. **Создание Интернет-Интерпола**
3. **Контроль за глобальной сетью**
4. **Усиление сотрудничества правоохранительных органов с антивирусными компаниями**

лаборатория КАСПЕРСКОГО

Спасибо за внимание!

Евгений Касперский

руководитель антивирусных исследований

eugene@kaspersky.com