

 KASPERSKY для бизнеса

Ключевые особенности и преимущества
Новых технологий

Региональный представитель в
УрФО и Пермском крае
Александр Орда

▶ **Ключевые тенденции**

Россиянус интернетус юзерус

Портрет типичного российского пользователя на основании данных 14,6 млн россиян за 2011 год



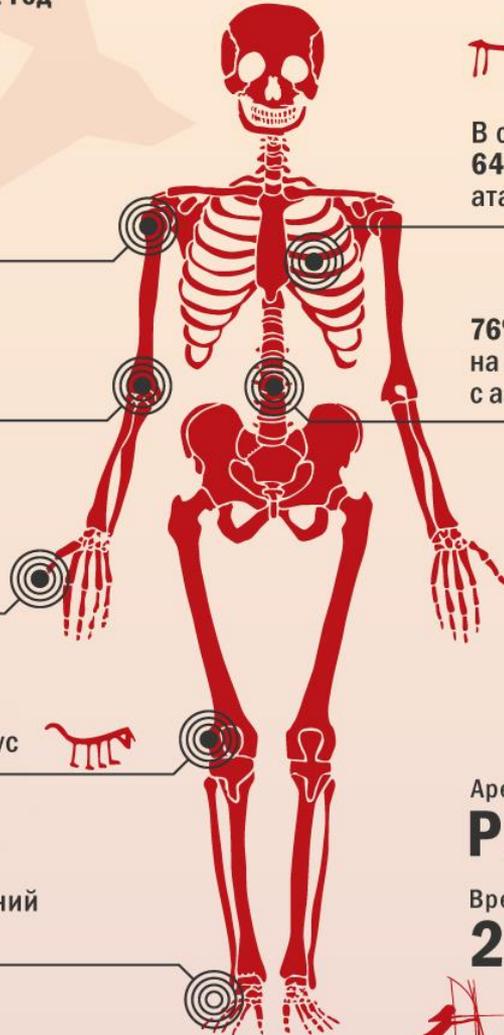
55% пользуются Windows XP

3/4 посещает сайты с вредоносным ПО

11 уязвимостей содержит в среднем каждый компьютер

У 56% хотя бы раз в год срабатывает веб-антивирус

В среднем на каждого приходится 36 срабатываний антивируса в год



В среднем каждый подвергается 64 сетевым и 10 фишинговым атакам в год

76% детей пытаются попасть на порносайты, 38% детей - на порталы с азартными играми



Ареал обитания

Россия

Время обнаружения

2011 год



Подвергается фишинговым атакам на поддельных сайтах, выдающих себя за



Подвергается попыткам заражения на сайтах, расположенных на территории



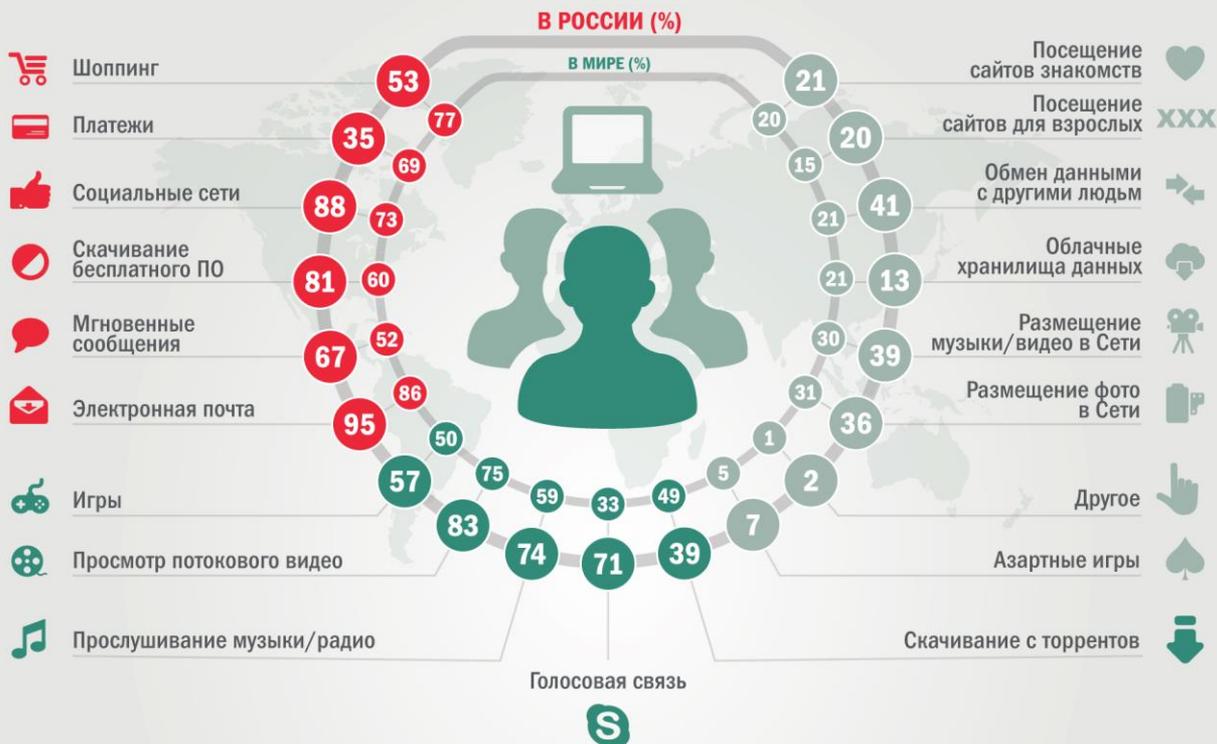
Попадает на сайты с вредоносным ПО через



▶ ТОП 5

Ежедневные активности пользователей в Интернете

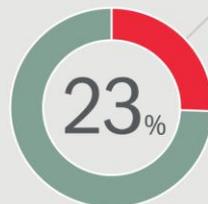
Российские пользователи оказались самыми активными во всём мире потребителями различных интернет-сервисов для общения



- ▶ Социальные Сети
- ▶ Электронная почта
- ▶ Просмотр потокового видео
- ▶ Развлекательные сайты.
- ▶ Голосовая связь

ВРЕДНОСНЫХ ХОСТИНГОВ

расположены в России (1-е место в мире).



РОССИЙСКИХ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЕЙ

сталкивались с риском заражения своих электронных устройств через Глобальную сеть (2-е место в мире).



▶ КЛЮЧЕВЫЕ ТЕНДЕНЦИИ

Планшеты и
мобильные
устройства

Усложнение
корпоративной
IT-инфраструктуры

Комплексные
угрозы

Зависимость
бизнеса от IT

Рост числа
угроз

Вирусы для
др. платформ

Мобильные
сотрудники

Вредоносное ПО для
смартфонов

BYOD

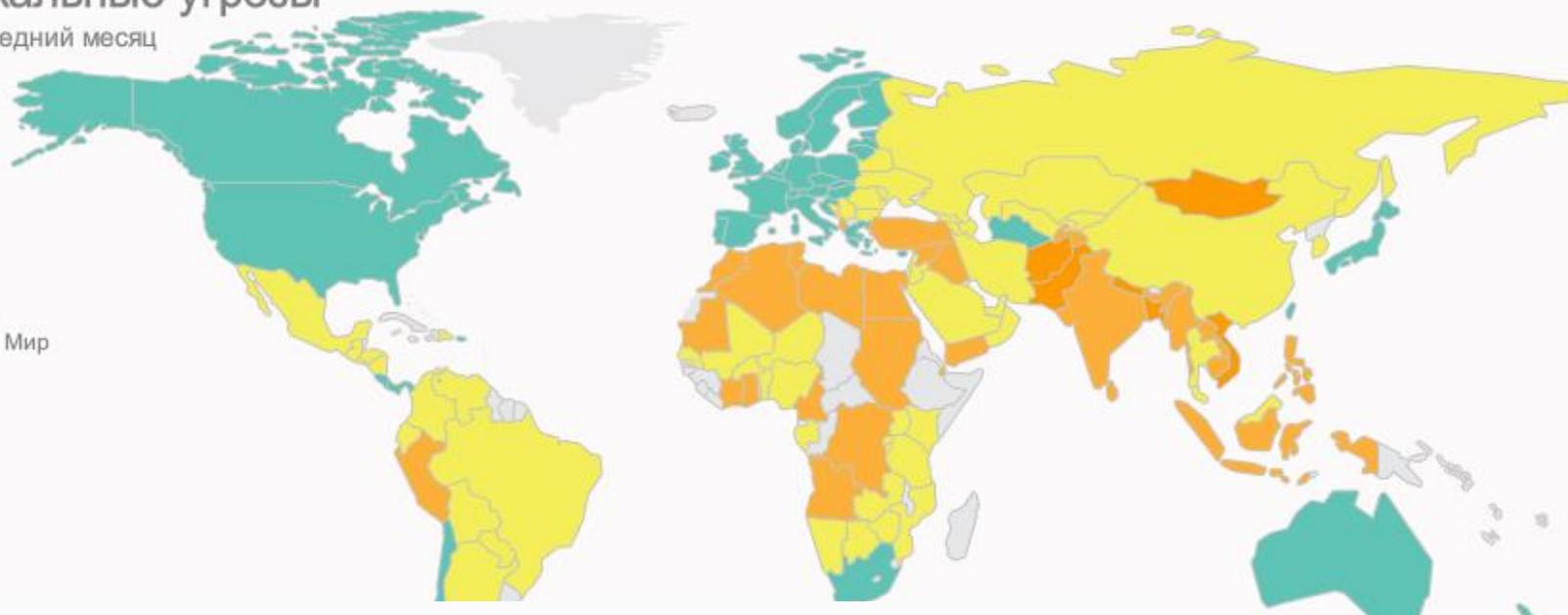
Облачные
сервисы и
виртуализация

Таргетированные
атаки

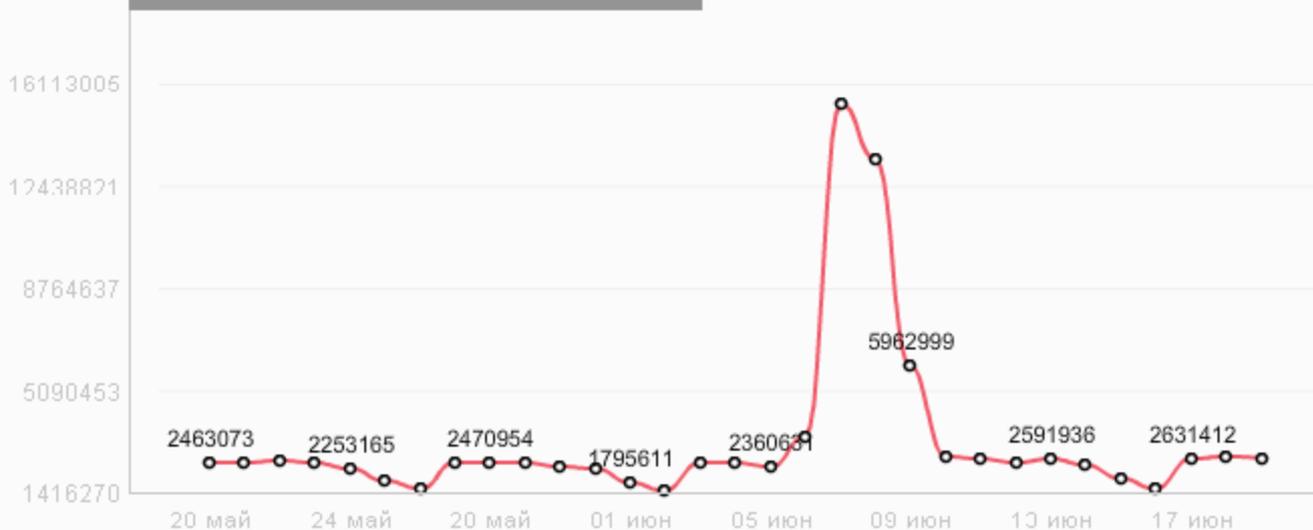
Локальные угрозы

Последний месяц

Мир



Локальные угрозы за месяц



Топ локальных угроз за месяц

1	Trojan.Win32.AutoRun.gen	19.3%
2	DangerousObject.Multi.Generic	16.7%
3	Trojan.Win32.Generic	12.6%
4	Exploit.Win32.CVE-2010-2568....	7.3%
5	Worm.Win32.Debris.a	6.2%
6	Virus.Win32.Sality.gen	5.6%
7	Trojan.WinLNK.Runner.ea	4.7%
8	Net-Worm.Win32.Kido.ir	3.5%
9	Virus.Win32.Nimnul.a	2.1%
10	Virus.Win32.Generic	2.1%

▶ ЧТО НОВОГО ?

▶ Botnet

▶ Социаль
инженер



В контакте

Главная

Валидация страницы

В течении 5 минут на Ваш мобильный телефон придет нужно ввести в форму ниже. Если Вы не получили от нас см можете отправить заявку на получение кода для вос доступа и подтверждения подлинности вашего аккаунта. , пожалуйста, следуйте детально инструкции:

Номер центра сертификации: **+79057599377**. Для подтвер подлинности вашего аккаунта необходимо:

- 1) Абонентам **МТС** необходимо ввести на телефоне бесплатный код, ***115#** . Выбрать **"Билайн"**, ввести **+79057599377**, ввести сумм платежа - 100 рублей и отправить запрос на проведение операции. После получения SMS-сообщения с просьбой подтвердить платек, отправить ответное SMS-сообщение с подтверждением запроса.
- 2) Абонентам **Билайн** необходимо набрать на телефоне команду ***145*9057599377*100#** и нажать кнопку вызова. Дождитесь SMS сообщения с кодом подтверждения. После чего наберите с Вашего мобильного телефона подтверждающую команду: ***145*[код подтверждения]#** и нажмите кнопку вызова.
- 3) Абонентам **Мегафон** и прочих операторов необходимо: пополнить счет **+79057599377** через терминалы оплаты на 100 рублей.

В ответном смс Вам придет код активации. Либо же воспользуйтесь кодом, указанным на чеке, полученном после платежа. После подтверждения кода, сумма снятая со счета будет обязательно возвращена в течении нескольких часов. Данная мера необходима для выявления спамерских аккаунтов и аккаунтов-пустышек для дальнейшего их удаления. **ВКонтакте всегда заботится о вашей безопасности!**

▶ ЧТО НОВОГО ?

- ▶ Botnet
- ▶ Социальная инженерия
- ▶ Мобильные злоумышленники
- ▶ Зловреды

▶ **ВАШ МОБИЛЬНИК ПОД УГРОЗОЙ ПРЯМО СЕЙЧАС**

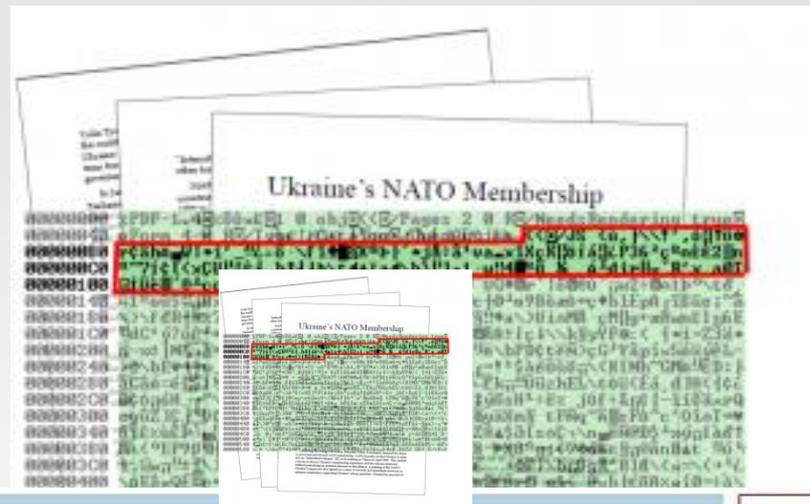


 [http://\[redacted\].ru/jimm.apk](http://[redacted].ru/jimm.apk)



▶ ЧТО НОВОГО ?

- ▶ Botnet
- ▶ Социальная инженерия
- ▶ Мобильные зловреды
- ▶ Возвращение «Старой Школы»



Edith Albert @EdithAlbert11
Albert, my cousin. He is working hard.
uri!wp07VkkxYmfNkwN2nBmx4ch/Iu2c+G
Jow39Hbph

Howard Fontenot @FontenotHoward
My native town was ruined by tornado.
uri!wp07VkkxYtgMd/JOnLhzRLzFjY8l2It

MiniDuke wird über spezielle Tweets gesteuert

▶ ЧТО НОВОГО ?

▶ Bot

▶ Со

ИНЖ

▶ Мо

зловреды

▶ Возвраще

«Старой Школы»

▶ Кибероружие



▶ Стоимость атаки снижается

WIRED.CO.UK

- ▶ DDoS атака: \$30-\$70 день, от \$1200 – месяц
- ▶ Рассылка SPAM: от \$10 за миллион адресов
- ▶ Боты для Бот сетей: от \$200 за 2000 Ботов
- ▶ Исходный код ZeuS: от \$200
- ▶ Взлом корпоративного почтового ящика: от \$500



▶ Как противостоять?

- ▶ Здравый смысл
- ▶ Самоконтроль
- ▶ Знания
- ▶ Использовать продукты Kaspersky Lab 😊



Сервисы



KDP – KASPERSKY DDoS PREVENTION

▶ DDoS – кому это нужно?

- ▶ Конкурентная борьба
- ▶ Вымогательство
- ▶ Мошенничество
- ▶ Месть

- ▶ Недовольство клиентов
- ▶ Недовольство контрагентов
- ▶ Недовольство Топ руководства
- ▶ Репутационный ущерб
- ▶ Срыв бизнес процессов
- ▶ Отвлечение от главного (хищения)
- ▶ Прямой ущерб (торговые площадки)

▶ Главное о KDP

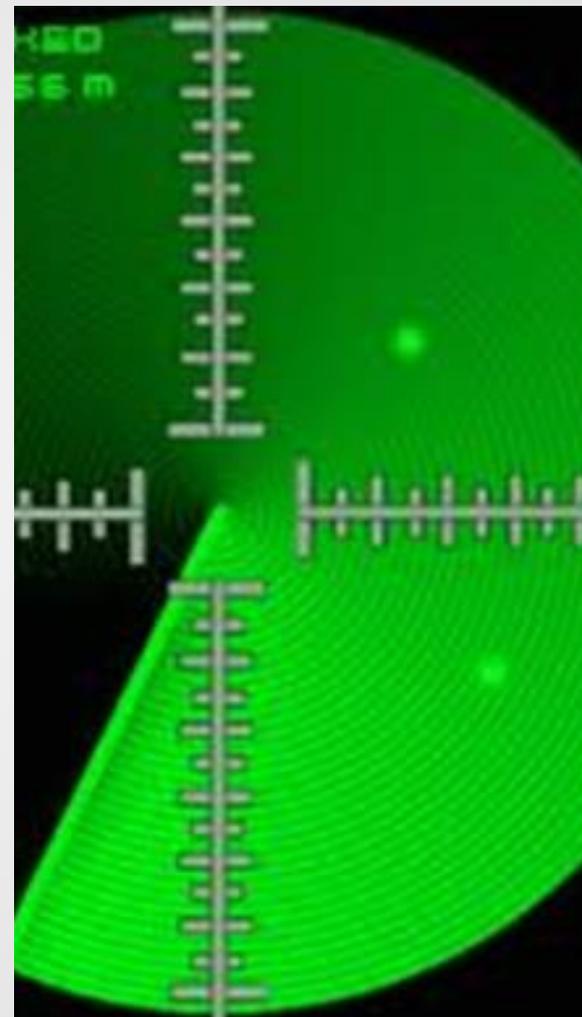
- ▶ Защита любых сервисов и приложений
- ▶ Собственная технологическая платформа
- ▶ 5 лет опыта
- ▶ Единое решение, не зависящее от текущих поставщиков Интернет-услуг
- ▶ Глобальная распределенная система фильтрации
- ▶ Внедрение без инфраструктурных изменений
- ▶ Мониторинг аномалий в режиме 24\7
- ▶ Аналитическое сопровождение атаки



Расследование Компьютерных Инцидентов

▶ Кого и зачем атакуют?

- ▶ Цели атаки
 - Экономические мотивы
 - Промышленный шпионаж, доступ к интеллектуальной собственности
 - Приостановка/создание препятствий для нормальной деятельности (саботаж)
- ▶ Большие и известные компании остаются основными целями
- ▶ Средние и маленькие компании атакуют все чаще, в том числе, для доступа к большим
 - до 40% атак – компании до 250 человек



▶ Как понять, что есть проблема?

- ▶ Подозрительные события в логах системных событий
- ▶ Подозрительные файлы в системном каталоге
- ▶ Большая сетевая и CPU загрузка
- ▶ Неизвестный трафик на подозрительные URL-ы
- ▶ Перестают обновляться AV сигнатуры, блокируются обновления ОС или Group Policy...



▶ Что мы делаем

- ▶ Выезжаем на место инцидента и собираем свидетельства
- ▶ Проводим цифровой криминалистический анализ
- ▶ Фиксируем результаты в юридически значимой форме
- ▶ Даем рекомендации по ликвидации последствий
- ▶ Находим лиц, причастных к инциденту
- ▶ Взаимодействуем с правоохранительными органами в рамках следствия и уголовного дела



Спасибо

Вопросы?



Региональный представитель в УрФО и
Пермскому краю
Александр Орда