



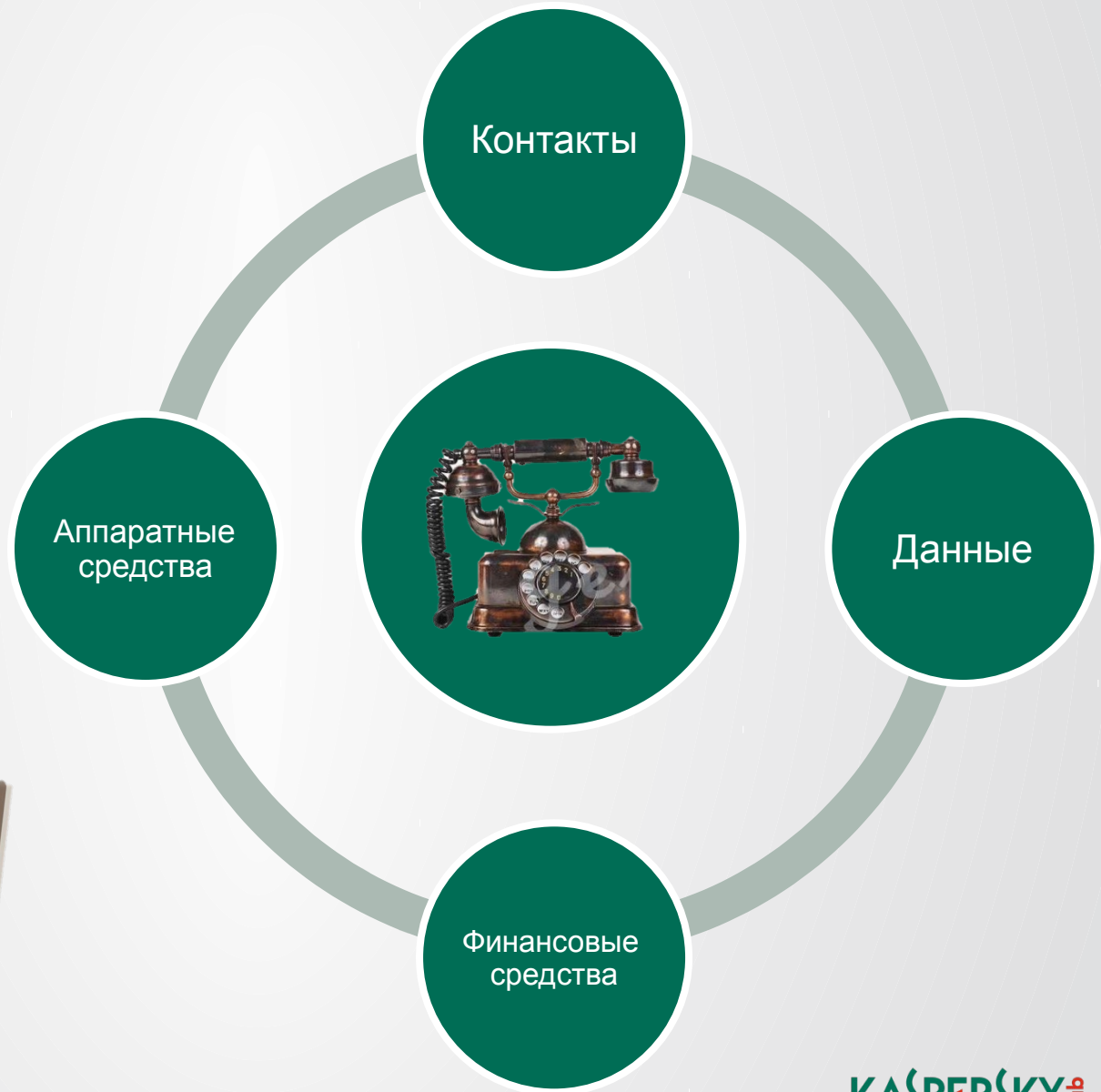
Защита на опережение

Развитие информационных угроз в 2012 году.
Решения Лаборатории Касперского.

Докладчик : Булат Сираев, консультант-аналитик.

Вредоносное ПО для мобильных устройств

Почему мобильные устройства являются целью вирусописателей?



Количество обнаруженных модификаций вредоносного ПО для Android OS



Решение: Kaspersky Endpoint Security 8 для Smartphone

Основные преимущества:

Антивирусное ядро удостоенное многочисленных наград

Защита от всех актуальных угроз

Защита данных при потере или краже устройства

Фильтрация входящих вызовов и SMS

Простое развертывание и администрирование



DDos-атаки – серьезные риски для
бизнес-процессов!

Какие цели преследуются исполнителями DDoS-атак?

Государственные информационные системы:

- кибертерроризм
- попытка вмешательства во внутренние дела
- выражение недовольства
- нанесение экономического, имиджевого и другого ущерба.

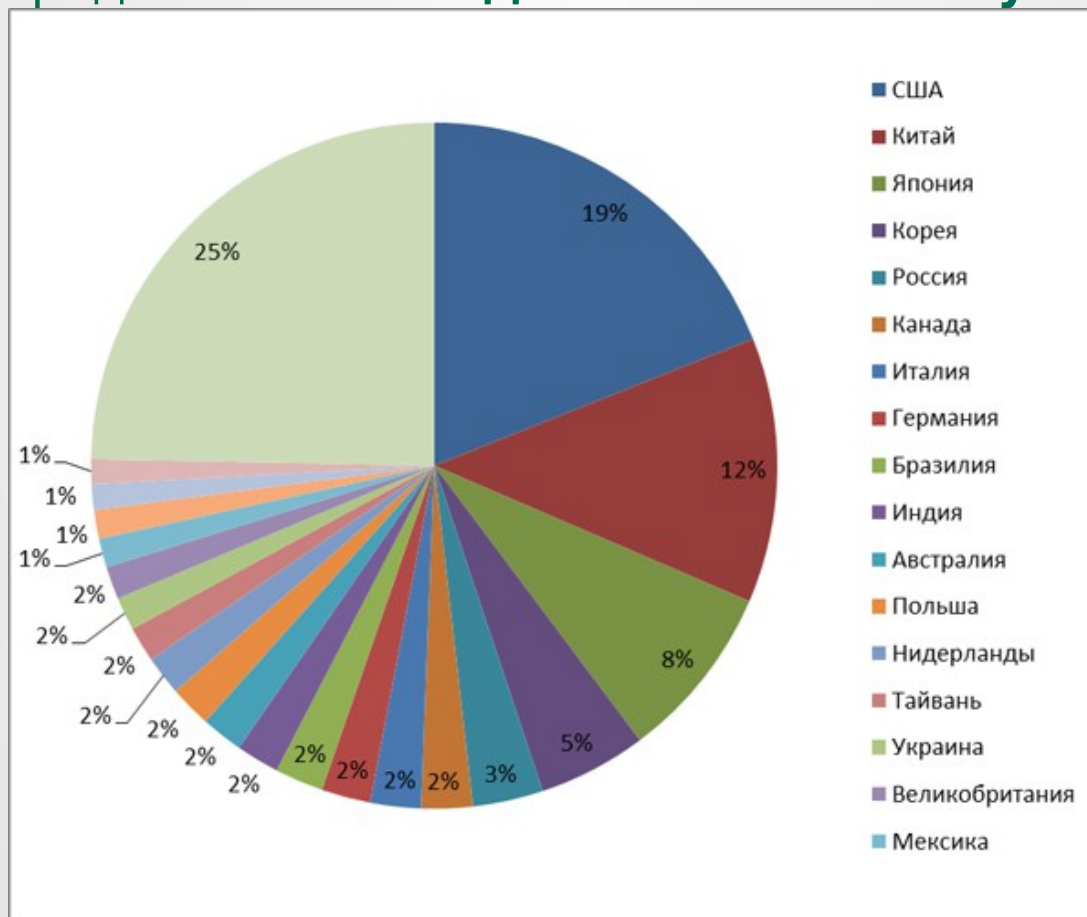
Корпоративные информационные системы:

- вымогательство
- конкурентная борьба
- месть
- прикрытие иных атак.

Статистика DDoS-атак в 2012 году.

Максимальная мощность атаки из числа отраженных Kaspersky DDoS Prevention составила **2,9 Гбит/с.**

Самая протяженная DDoS-атака, зафиксированная в первом полугодии, продолжалась **94 дня 4 часа 58 минут**



Почему неэффективна существующая защита?



Брандмауэры, системы IDS\IPS: находятся непосредственно перед защищаемым ресурсом и бессильны против атаки на переполнение канала связи;



Маршрутизация в «черные дыры»: применяется провайдерами и заключается в перенаправлении атакующего трафика. В процессе перенаправляются и легальные запросы, то есть, злоумышленники достигают своей цели — ресурс становится недоступным для пользователей



Правильная настройка системы: помогает только от небольших и плохо подготовленных атак



Резервирование ресурсов - неэффективный и дорогой метод.

Решение: Kaspersky DDoS Prevention

Основные преимущества:

Построение статистического профиля по трафику конкретного ресурса, что обеспечивает индивидуальную защиту.

Услугой Kaspersky DDoS Prevention можно воспользоваться как заранее, для предотвращения атаки, так и после того, как она уже началась.

Сервис KDP не зависит от какого-либо конкретного провайдера, что также повышает его надежность и отказоустойчивость.

Огромный опыт «Лаборатории Касперского» в борьбе с бот-нетами, без которых невозможно проведение сколько-нибудь крупных DDoS-атак.

Аналитики «Лаборатории Касперского» помогут подготовить пакет документов, необходимый для обращения в правоохранительные органы.

Спасибо!