ЦЕНТР ИССЛЕДОВАНИЙ И АНАЛИЗА УГРОЗ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

Илья Кудрин

АО «Лаборатория Касперского»

ЭВОЛЮЦИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Взгляд назад: 20 лет эволюции вредоносных программ

МАСШТАБ УГРОЗЫ

1994

1

НОВЫЙ ВИРУС КАЖДЫЙ ЧАС

2006

1

НОВЫЙ ВИРУС КАЖДУЮ МИНУТУ

2011

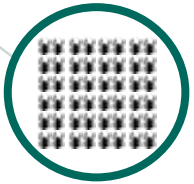
1

НОВЫЙ ВИРУС КАЖДУЮ СЕКУНДУ

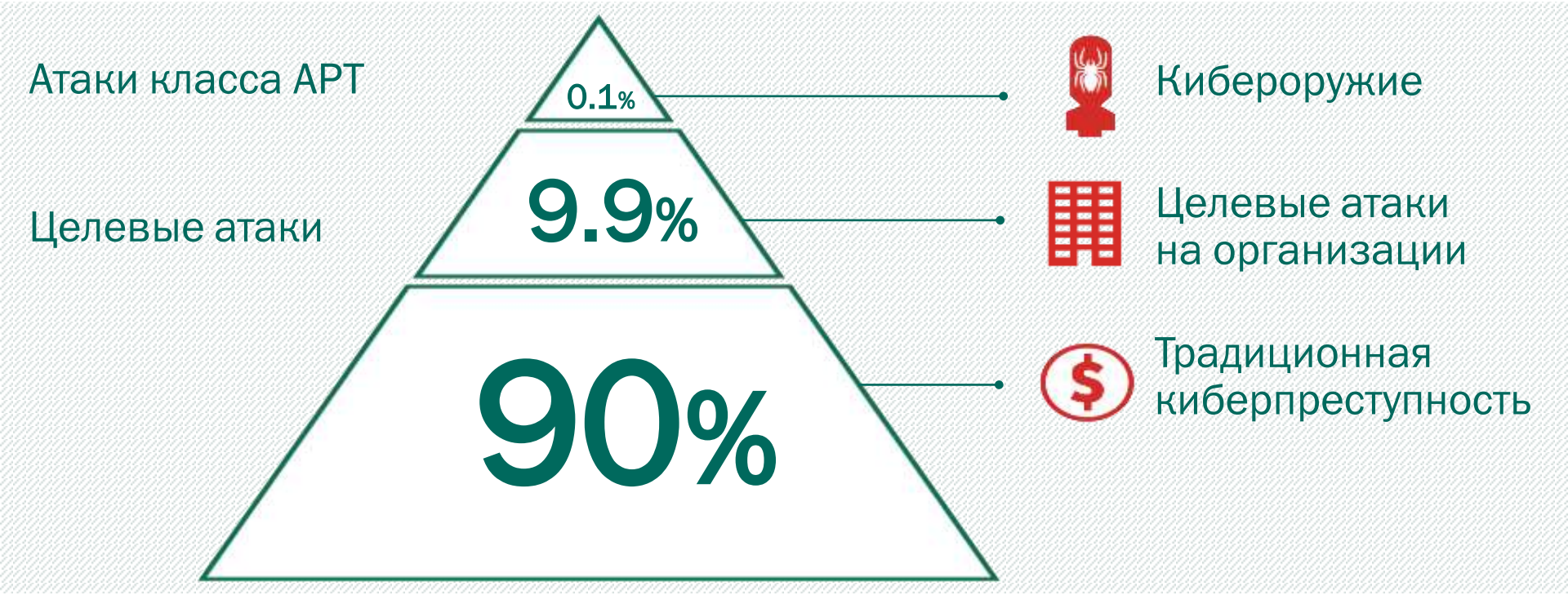
2015

310000

НОВЫХ ВРЕДОНОСНЫХ ОБРАЗЦОВ В ДЕНЬ



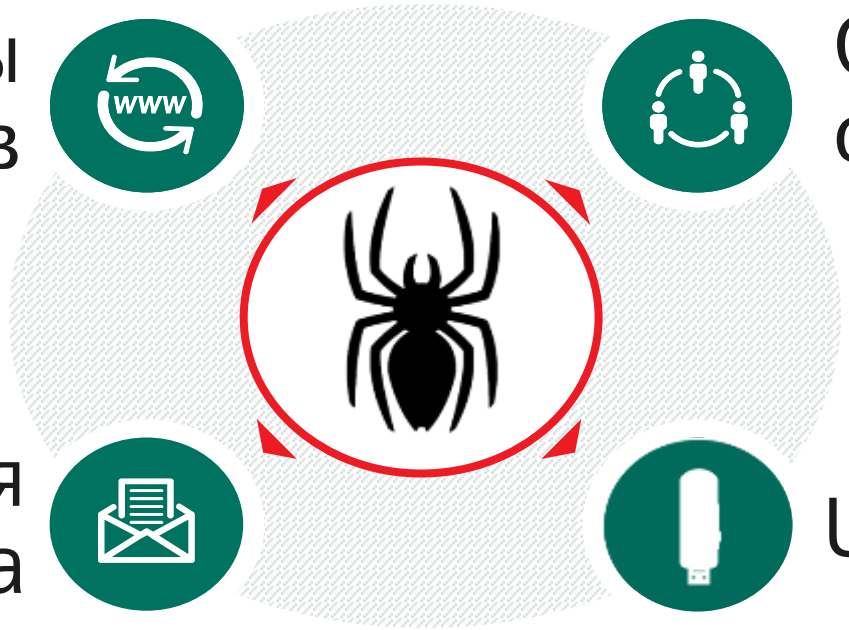
ВИДЫ УГРОЗ


Атаки класса APT
0.1%
Кибероружие
Целевые атаки
9.9%
Целевые атаки
на организации
90%
Традиционная
киберпреступность

КАК РАСПРОСТРАНЯЕТСЯ ВРЕДОНОСНОЕ ПО

Наборы эксплойтов

Социальные сети



Электронная почта

USB

ЭВОЛЮЦИЯ КИБЕРУГРОЗ: Q1 2016

Основные цифры и статистика

ОСНОВНАЯ СТАТИСТИКА: Q1 2016

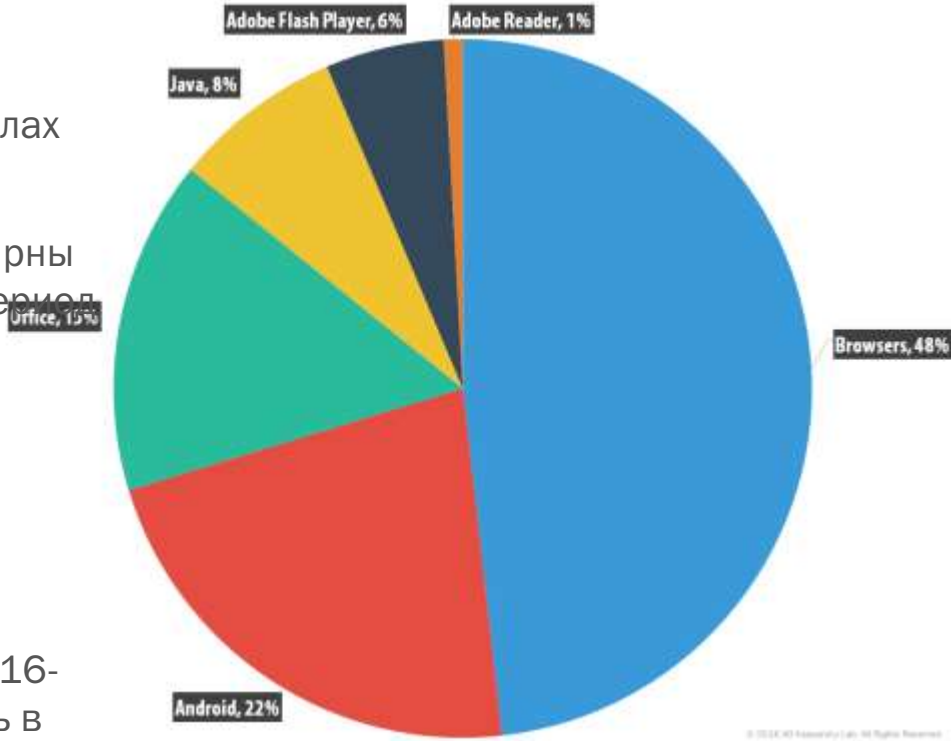
- Решения «Лаборатории Касперского» отразили **228.420.754 атак**, организованных с онлайн-ресурсов, расположенных по всему миру.
- Компоненты сетевой защиты признали вредоносными **74.001.808 уникальных URL**.
- Атаки программ-шифровальщиков и вымогателей заблокированы на **372.602** компьютерах уникальных пользователей.
- Решения «Лаборатории Касперского» для защиты мобильных устройств обнаружили:
  - **2.045.323** установочных пакета
  - **4.146** новых троянцев-вымогателей
  - **2.896** мобильных банковских троянцев

УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ КИБЕРПРЕСТУПНИКАМИ

- Верхняя позиция в первом квартале 2016 года досталась категории «Браузеры» (64%), которая включает эксплойты для веб-браузеров. Эта же категория лидировала и в последних трех кварталах 2015 года.

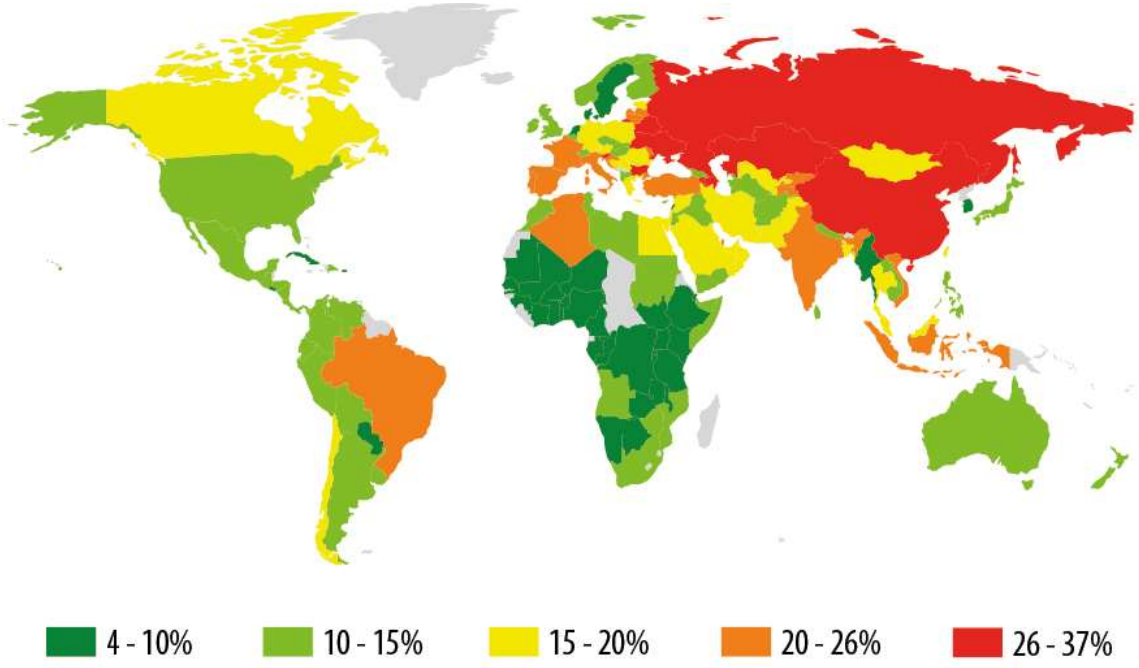
- В первом квартале 2016 года оставались популярны эксплойты под Adobe Flash Player. За отчетный период было обнаружено две новых уязвимости:
  CVE-2015-8651
  CVE-2016-1001
  Первым эксплойт-паком, поддерживающим эти уязвимости, оказался Angler.

- Заметной тенденцией первого квартала стало использование эксплойта для Silverlight - CVE-2016-0034. На момент эта уязвимость использовалась в эксплойт-паках Angler и RIG.



СТРАНЫ, ГДЕ ПОЛЬЗОВАТЕЛИ ПОДВЕРГАЮТСЯ НАИБОЛЬШЕМУ РИСКУ ЗАРАЖЕНИЯ ОНЛАЙН

- Лидер остается неизменным – это Россия, с показателем 36,3%. С прошлого квартала Чили, Монголия, Болгария и Непал покинули первую 20-ку стран. А в числе новичков оказались Словения (26,9%), Индия (24%) и Италия (23%).

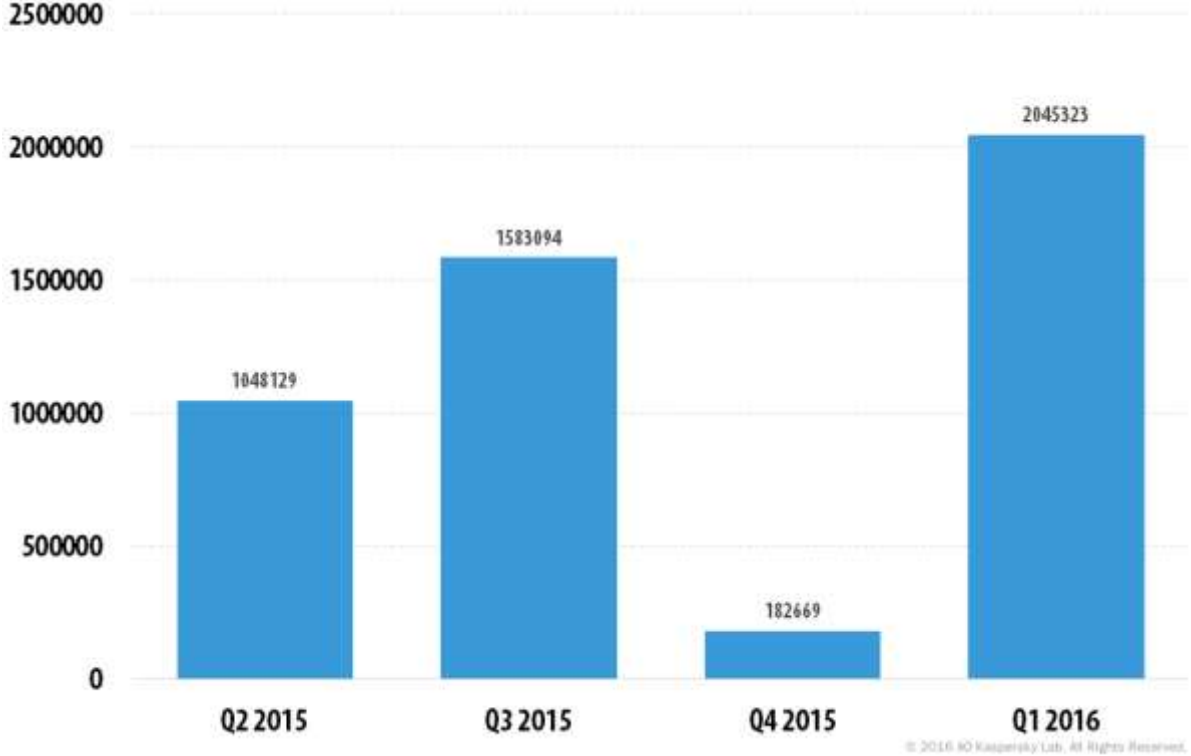


МОБИЛЬНЫЕ УГРОЗЫ: Q1 2016

Основные цифры и статистика

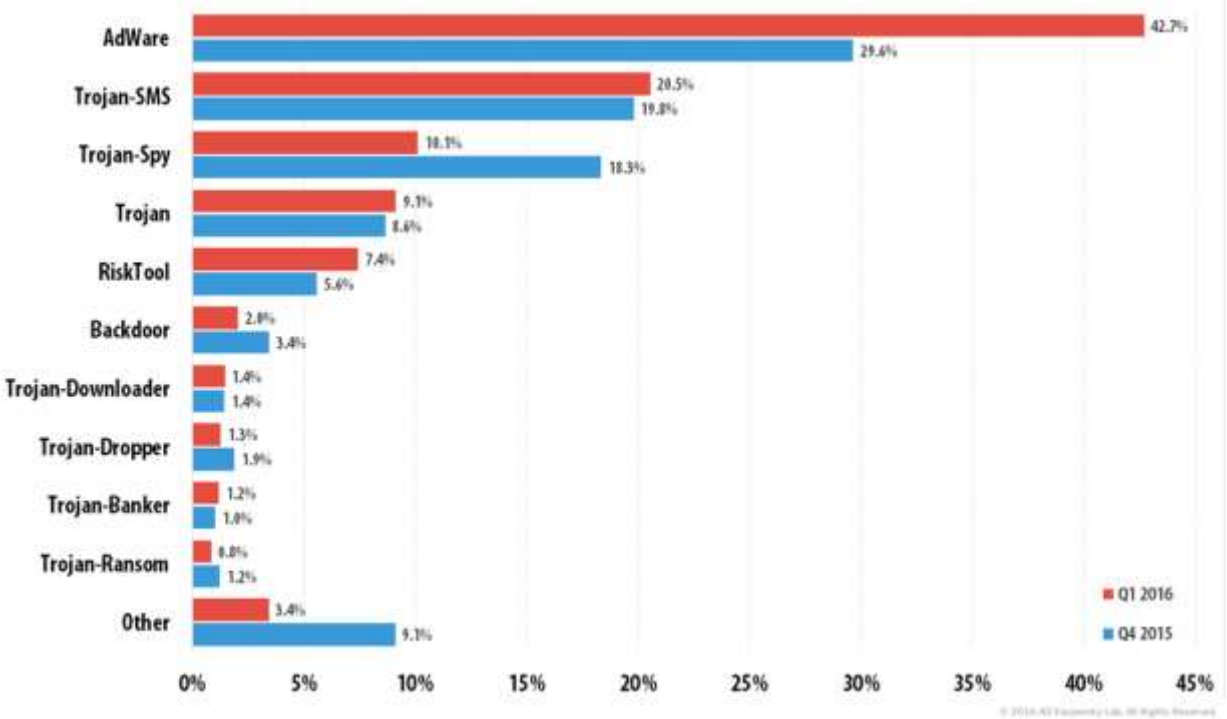
МОБИЛЬНЫЕ УГРОЗЫ
ОСНОВНАЯ СТАТИСТИКА Q1 2016

«Лаборатория Касперского» обнаружила 2.045.323 вредоносных установочных пакета – это в 11 раз больше, чем в четвертом квартале 2015 г., и в 1,2 раза больше, чем в третьем квартале 2015 г.



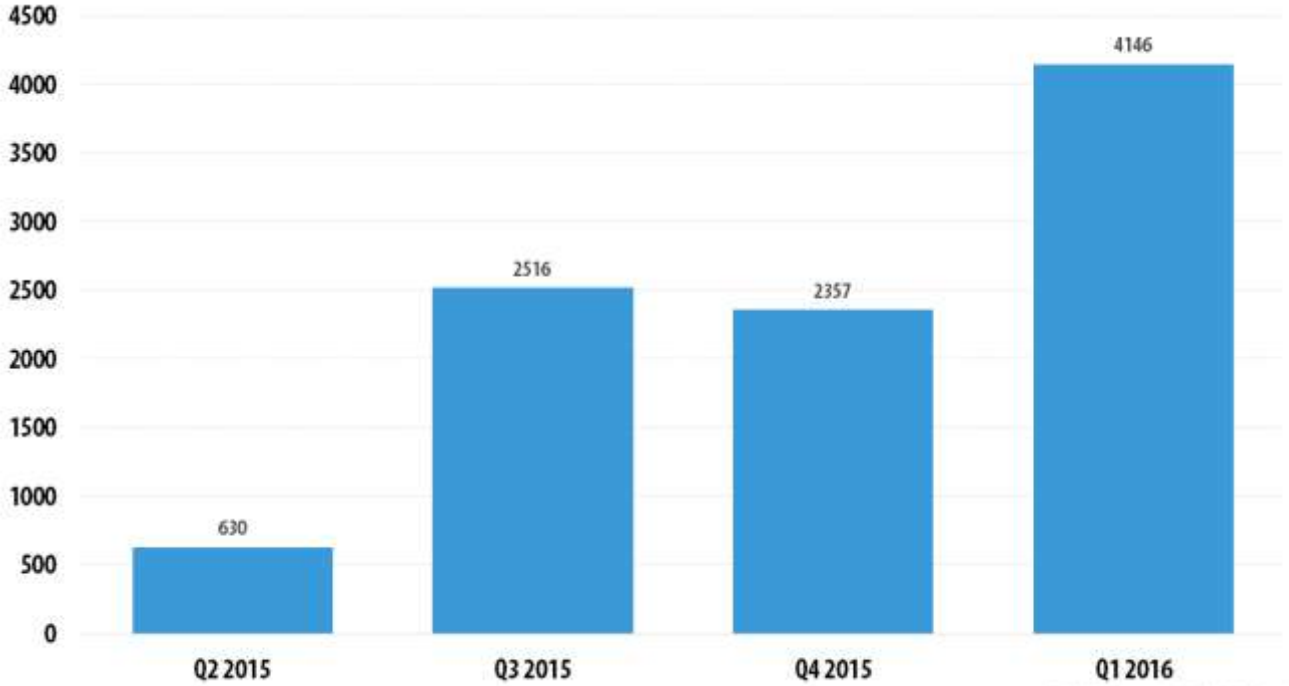
МОБИЛЬНЫЕ УГРОЗЫ
ОСНОВНАЯ СТАТИСТИКА Q1 2016

В первом квартале 2016 года рекламное ПО продолжало возглавлять рейтинг обнаруженных вредоносных объектов для мобильных устройств. Доля рекламного ПО выросла на 13 процентных пункта по сравнению с четвертым кварталом 2015 года и составила 42,7%. Примечательно, что это ниже, чем в третьем квартале 2015 года (52,5%).



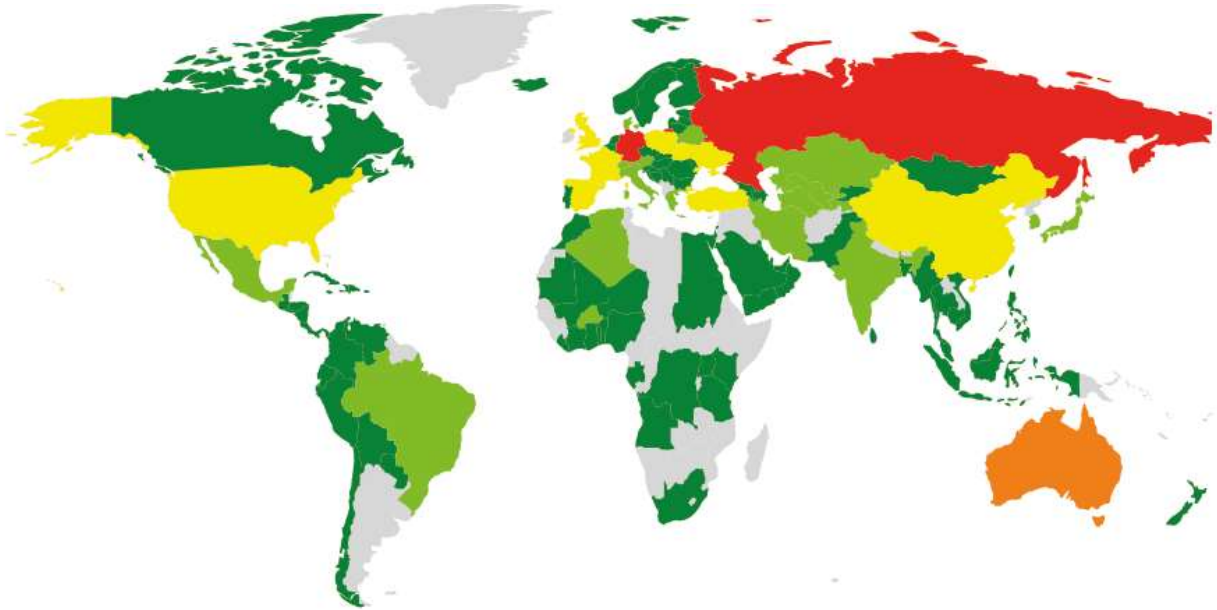
МОБИЛЬНЫЕ БАНКОВСКИЕ ТРОЯНЦЫ

В отчетном периоде мы обнаружили 4.146 мобильных банковских троянцев, что в 1,7 раза больше, чем в предыдущем квартале. (процент от всех атакованных пользователей)



МОБИЛЬНЫЕ БАНКОВСКИЕ ТРОЯНЦЫ - ГЕОГРАФИЯ

- География мобильных банковских троянцев в первом квартале 2016 года. (число атакованных пользователей)



ВРЕДОНОСНОЕ ПО – ИНЦИДЕНТЫ

Актуальные проблемы

ШИФРОВАЛЬЩИКИ – ПРОБЛЕМА ГОДА?

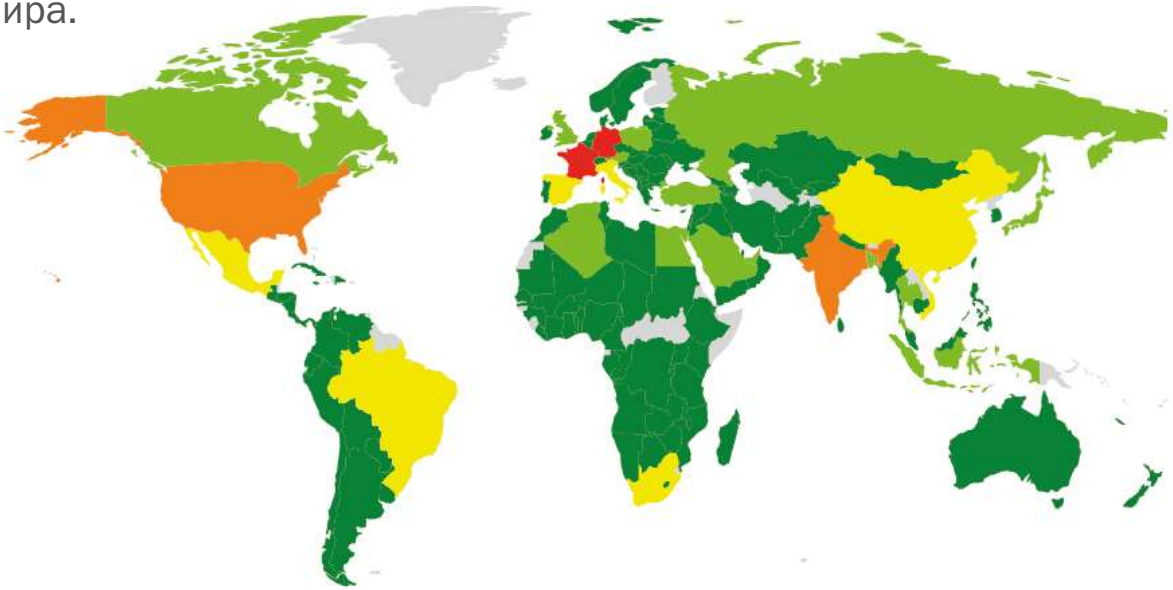
За первые три месяца 2016 года произошло такое количество киберинцидентов, которое несколько лет назад считалось бы нормой для целого года. Основные тенденции остаются теми же, однако мы видим рост в трендах, имеющих отношение к традиционной киберпреступности, особенно в том, что касается мобильных угроз и шифровальщиков, которые заполонили весь мир.

Шифровальщики стали основной темой квартала, сместив с лидерских позиций целевые атаки. К сожалению, эта ситуация продолжит развиваться быстрыми темпами и те, кто стоит за вымогательством, с легкостью могут быть названы «проблемой года».

ШИФРОВАЛЬЩИКИ – LOCKY

- Наибольшее число инцидентов с шифровальщиками в первом квартале 2016 года спровоцировал троянец Locky.

- Решения «Лаборатории Касперского» зафиксировали попытки заражения пользователей в 114 странах мира.



ШИФРОВАЛЬЩИКИ – PETYA

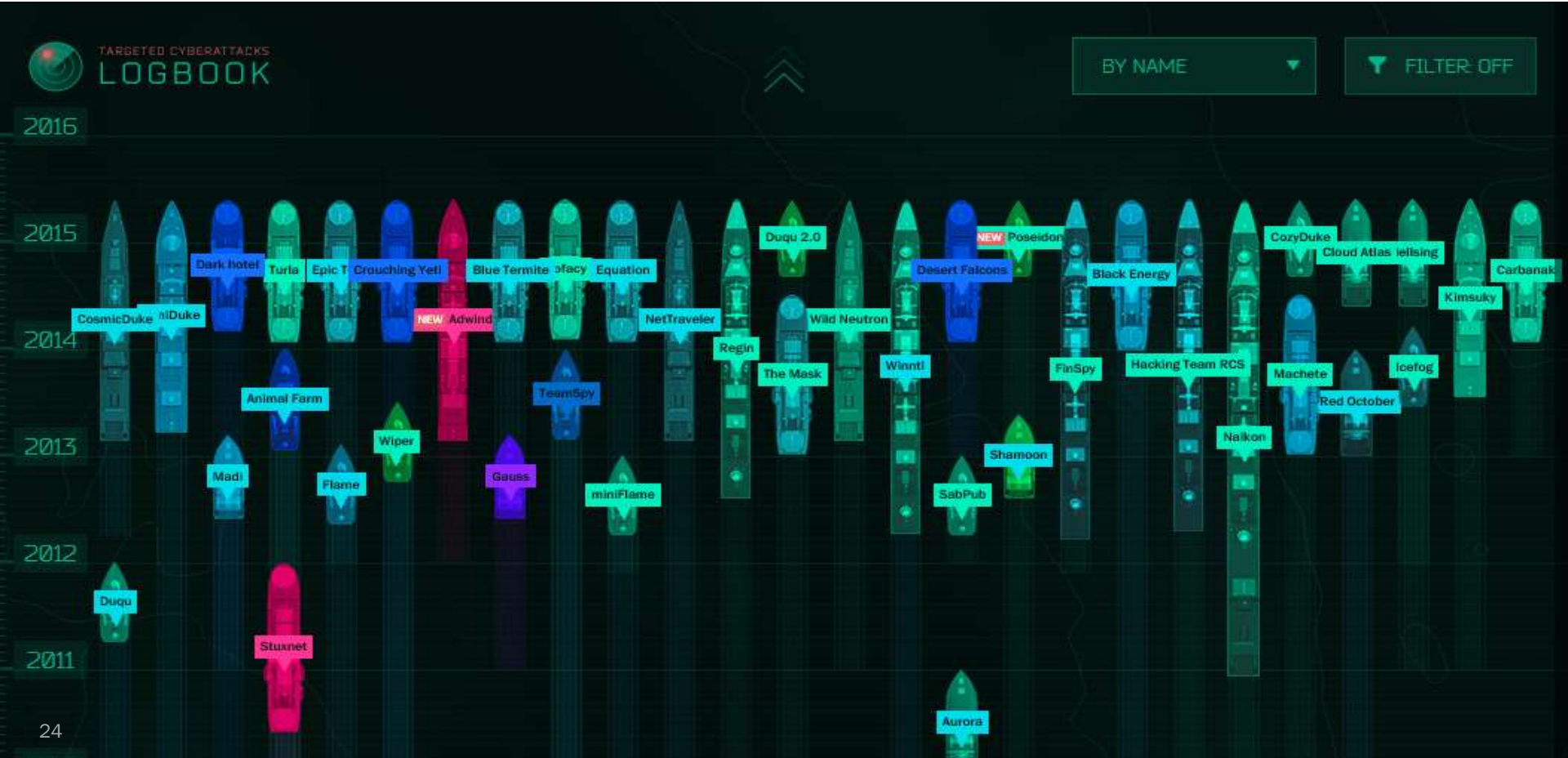
- Наиболее значительной инновацией в технологии шифровальщиков стало полное шифрование диска, а не каждого отдельного файла. Именно этот прием был использован троянцем Petya.

- Завершив шифрование таблицы главного файла, Petya показывает свое настоящее лицо – череп с перекрещенными костями, состоящие из символов таблицы кодировки ASCII. А затем все как всегда: троянец требует от жертвы заплатить выкуп, который в данном случае составляет 0,9 биткойна (около $380).

ЦЕЛЕВЫЕ АТАКИ

Текущая ситуация

ЦЕЛЕВЫЕ АТАКИ И АТАКИ КЛАССА APT БЫСТРО РАСТУТ



ЦЕЛЕВЫЕ АТАКИ – POSEIDON

Poseidon – первая португалоговорящая кибергруппировка, создавшая своего рода бутик кастомизированного вредоносного ПО.

Группировка была активна в течение долгого времени. Вредоносные кампании, которые с большой вероятностью поддерживались Poseidon, были обнаружены еще в 2005 году, а первые образцы датируются 2001 годом.

Цель атаки – контроллер локального домена Windows. Как только атакующие получают доступ к нему, они могут красть интеллектуальную собственность, данные, информацию, составляющую коммерческую тайну, или любые другие ценные данные.

В большинстве случаев использовалась с **целью шантажа** пострадавших организаций и навязывания услуг Poseidon в качестве консультанта по безопасности. Вне зависимости от того, соглашалась ли жертва на такие условия, Poseidon все равно оставался в сети.

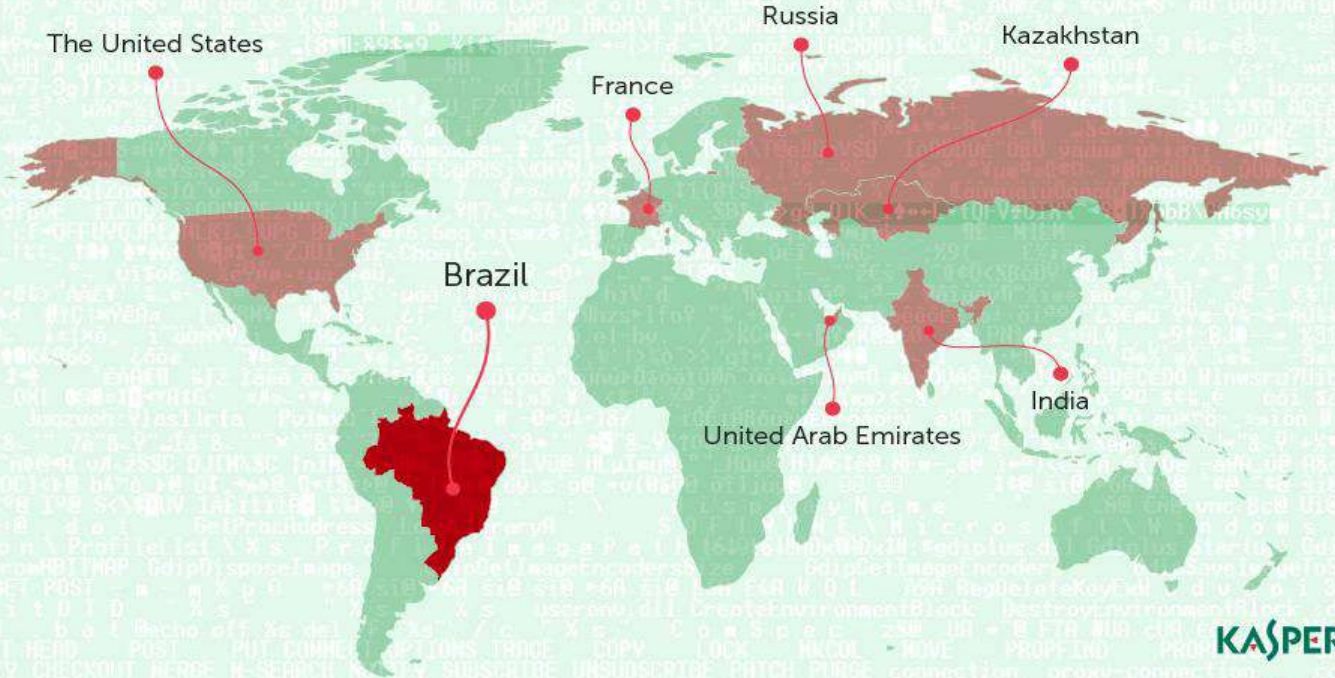
Poseidon's Targeted Attacks Malware Boutique

The targets of the Poseidon cyberespionage group

Energy and utilities | Financial institutions | Governmental | Public relations and media | Manufacturing | Natural resources | Services

English and Portuguese.

The first ever Brazilian Portuguese speaking targeted attack campaign



Evolving their toolkit since at least 2005, active at this time

KASPERSKY lab

ЦЕЛЕВЫЕ АТАКИ – «ЗЛОВРЕД КАК УСЛУГА» ADWIND

Троянец развивался поэтапно в течение нескольких лет. Первые его образцы появились в 2012 году. Зловред имел разные имена: в 2012-м вирусописатели продавали его под названием Frutas, в 2013-м он именовался Adwind, в 2014-м стал известен как Unrecom и AlienSpy, а в 2015-м получил имя JSocket.

Основные пользователи этого троянца – организаторы хорошо подготовленных мошеннических операций, нечестные конкуренты, а также кибернаемники, получающие деньги за онлайн-слежку за людьми и организациями. Однако Adwind может воспользоваться любой, кто хочет проследить за своими друзьями.

Расследование имело последствия: спустя несколько дней после публикации отчета сайт JSocket перестал работать, а авторы Adwind свернули свою активность. С тех пор новые версии троянца не появлялись. Возможно, нам следует ожидать очередной реинкарнации зловреда, а, может быть, это конец истории.

Жертвы Adwind – «зловреда как услуги»

В процессе расследования эксперты «Лаборатории Касперского» проанализировали около 200 случаев целенаправленных фишинговых атак, организованных неизвестными киберпреступниками для распространения Adwind.

Исходя из данных, полученных с помощью облачной инфраструктуры Kaspersky Security Network, эти 200 атак затронули более **68000** пользователей в период с августа 2015 года по январь 2016-го.

* Топ-10 наиболее часто атакуемых стран в период с августа 2015 по январь 2016.

GREAT KASPERSKY lab

KASPERSKY lab

ЦЕЛЕВЫЕ АТАКИ – БАНКОВСКИЕ УГРОЗЫ

На конференции Security Analyst Summit «Лаборатория Касперского» объявила об обнаружении двух новых группировок Metel и GCMAN, вовлеченных в ограбления банков при помощи атак класса APT, а также о возобновлении активности группы Carbanak.

В 2015 году эксперты «Лаборатории Касперского» провели расследование для 29 российских организаций в ответ на инциденты, за которыми стояли эти три группировки.

Деятельность Carbanak 2.0 представляет особенный интерес. В декабре 2015 года «Лаборатория Касперского» подтвердила, что группировка все еще активна – подтверждением тому стали следы Carbanak в телекоммуникационной компании и финансовой организации. Интересной особенностью группы Carbanak 2.0 является то, что они выбрали новый тип жертв: теперь злоумышленники атакуют бухгалтерии любых организаций, представляющих для них интерес. Но они по-прежнему используют инструменты и техники, характерные для атак класса APT.

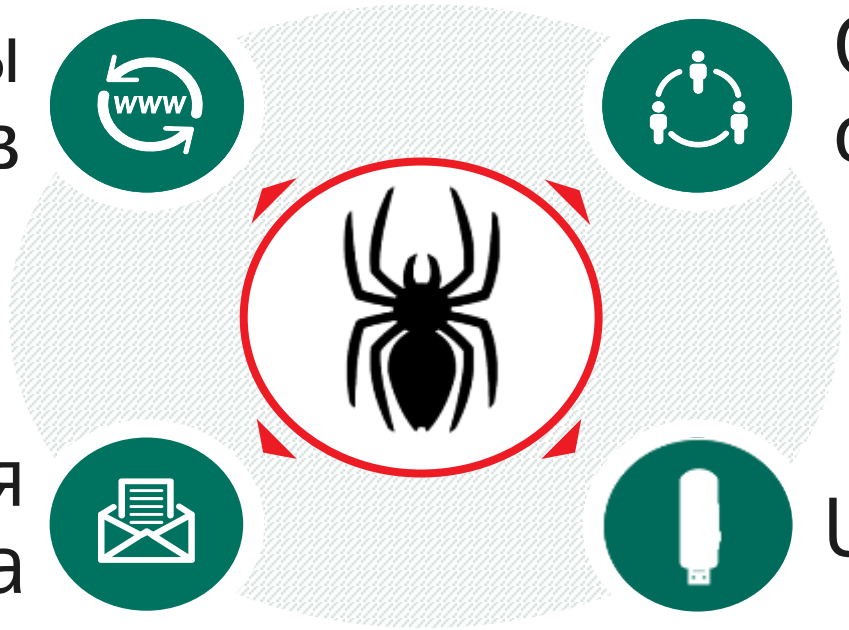
Как преступник группировки Carbanak атакует финансовые организации

KASPERSKY lab

КАК РАСПРОСТРАНЯЕТСЯ ВРЕДОНОСНОЕ ПО

Наборы эксплойтов

Социальные сети



Электронная почта

USB

ПРОСТЫЕ ПРАВИЛА

- Делать сложные пароли
- Для покупок в интернете завести отдельную карту
- Проверять ссылки по которым переходим
- Не хранить в телефоне данные платежных карт
- Не выкладывать в Соцсети лишнюю информацию
- Не открывать вложения если есть сомнения в источнике их отправки

KASPERSKY ENDPOINT SECURITY CLOUD

KASPERSKY lab

МАЛЫЙ И СРЕДНИЙ БИЗНЕС: ЗАДАЧИ И СЛОЖНОСТИ

Требования к безопасности похожи у компаний любой величины

- Защита конфиденциальных данных
- Непрерывность бизнес-процессов
- Безопасность мобильных устройств

Сложности, присущие малому и среднему бизнесу

- Ограниченное время на IT-безопасность
- Недостаточно ресурсов на администрирование сложных решений
- Скромные (по сравнению с крупными корпорациями) IT-бюджеты

KASPERSKY ENDPOINT SECURITY CLOUD: ПРЕИМУЩЕСТВА

Признанные технологии мирового уровня

Централизованное управление

Полностью готовое к работе решение

Отсутствие дополнительных инфраструктурных затрат

ЦЕНТРАЛИЗОВАННОЕ ОБЛАЧНОЕ УПРАВЛЕНИЕ ДЛЯ ВСЕХ ВИДОВ УСТРОЙСТВ

Единая консоль

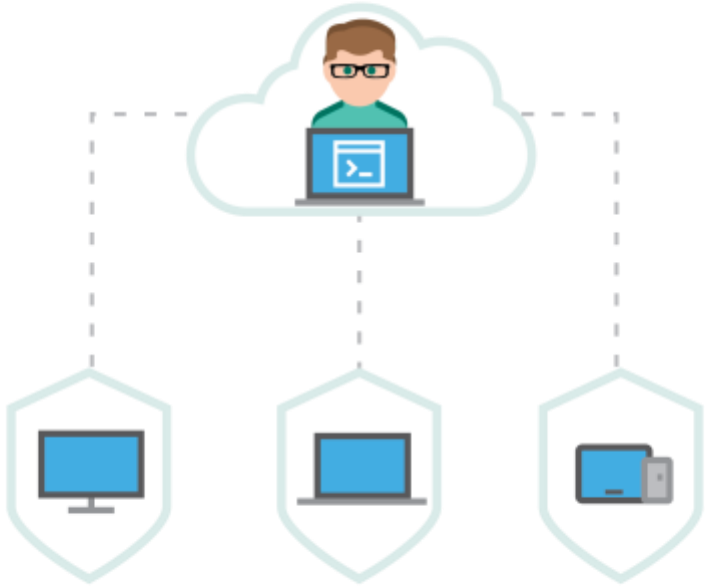
Централизованная контроль для управления защитой различных устройств: рабочих станций, файловых серверов и мобильных устройств.

Немедленная защита

Предустановленные политики помогут защитить вашу организацию сразу после развертывание решения.

Безопасность пользователей, а не устройств

Политики безопасности автоматически применяются ко всем устройствам пользователя, независимо от их типа и платформы.



KASPERSKY

ГОТОВОЕ РЕШЕНИЕ

Удаленное управление

Облачная консоль управления доступна из любой точки мира по адресу cloud.kaspersky.com.

Быстрое развертывание

Уже через несколько минут решение начнет работу. В то же время развертывание локально установленных решений занимает несколько часов или даже дней.

Пробный период – 30 дней

Полнофункциональная версия решения доступна бесплатно в течение 30 дней

ОТСУТСТВИЕ ДОПОЛНИТЕЛЬНЫХ РАСХОДОВ

Не нужно покупать серверы и ПО

«Лаборатория Касперского» уже позаботилась обо всех необходимых инфраструктурных элементах – все нужное для защиты вашего периметра находится в облачной консоли.

Не нужно проходить тренинги

Управление решением реализовано максимально просто, вам не потребуются специфические технические навыки.

Не нужно тратить много времени на управление

Даже если у вас есть только 15 минут в неделю, чтобы управлять системой IT-безопасности, Kaspersky Endpoint Security Cloud обеспечит надежную защиту вашей организации.

КАК РАБОТАЕТ РЕШЕНИЕ?

Поддерживаемые платформы

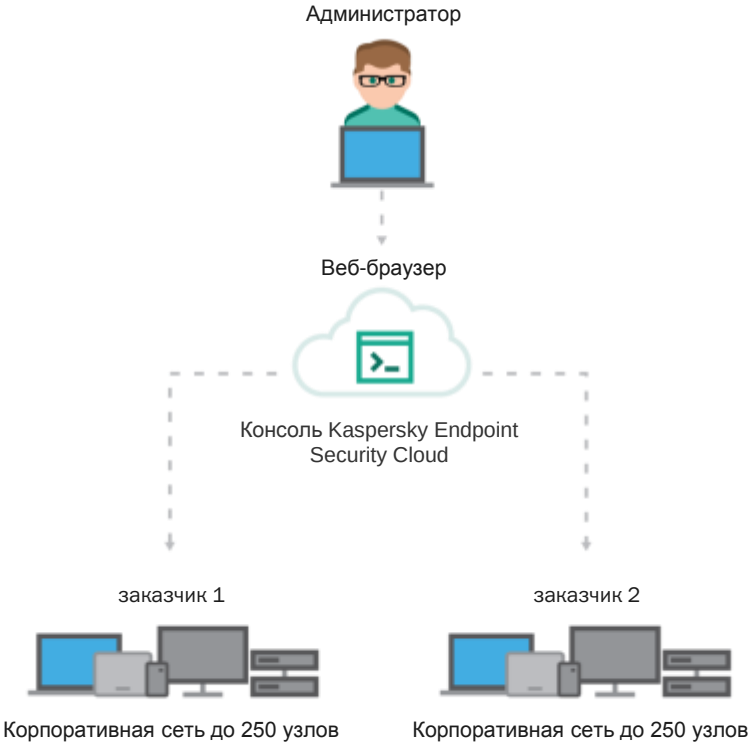
- Компьютеры и ноутбуки на базе Windows
- Файловые серверы Windows
- Смартфоны и планшеты Android и iOS

Централизованная панель управления

- Создание и настройка политик безопасности
- Проверка статуса защиты корпоративной сети и получение статистики о защите рабочих мест
- Отслеживание числа лицензий

Одна консоль для управления множеством сетей (по требованию)

- Защита до 250 узлов в каждой из сети



ФУНКЦИОНАЛЬНОСТЬ ПРОДУКТА

РАБОЧИЕ СТАНЦИИ И ФАЙЛОВЫЕ СЕРВЕРЫ НА БАЗЕ WINDOWS		
ЗАЩИТА	Защита от вредоносного ПО	✓
	Сетевой экран	✓
	Веб-защита	✓
	Почтовый антивирус	✓
	Мониторинг системы	✓
	Блокировщик сетевых атак	✓
СРЕДСТВА КОНТРОЛЯ	Веб-Контроль	✓
	Контроль устройств	✓

СМАРТФОНЫ И ПЛАНШЕТЫ		Android	iOS
SECURITY	Защита от вредоносного ПО	✓	✗
	Анти-Фишинг / Безопасный браузер	✓	✓
	Фильтрация звонков и SMS	✓	✗
	Настройки пароля	✓	✓
MDM	Настройка корпоративной почты	✓	✗
	Контроль Wi-Fi и Bluetooth	✓	✗
	Контроль встроенной камеры	✓	✓
	Анти-Вор (удаленные блокировка/стирание данных)	✓	✓
	Управление функциями iOS	N/A	✓

KASPERSKY ENDPOINT SECURITY CLOUD

Kaspersky Endpoint Security Cloud.

ДРУГОЙ УРОВЕНЬ УПРАВЛЕНИЯ

Попробуйте на cloud.kaspersky.com

ВОПРОСЫ?

Илья Кудрин

Ilya.kudrin@kaspersky.com

+7 343 271 9 271

KASPERSKY lab