Отчет Cisco

по кибербезопасности за первое полугодие 2016 г.

Алексей Лукацкий

Cisco Security

Мы продолжаем наши исследования

cisco

Взгляд на глобальную телеметрию Cisco

- 16 млрд интернет-запросов в день
- 600 млрд электронных сообщений в день
- Блокирование почти 20 млрд угроз в день
  - Более 1,5 млн уникальных образцов вредоносного ПО в день (17 в секунду)
  - На каждого жителя Земли приходится по 3 угрозы в день!
- 18,5 млрд запросов AMP
  - 214 тыс. запросов AMP в секунду

Асимметричная война: приемы киберпреступников превосходят нашу обороноспособность

- Инновационные методы
- Постоянные атаки
- Меняющаяся тактика
- Глобальный масштаб действий

Рост числа уязвимостей

Слабая инфраструктура

Дилемма шифрования

Чрезмерная нагрузка на специалистов по безопасности

cisco

Обзор

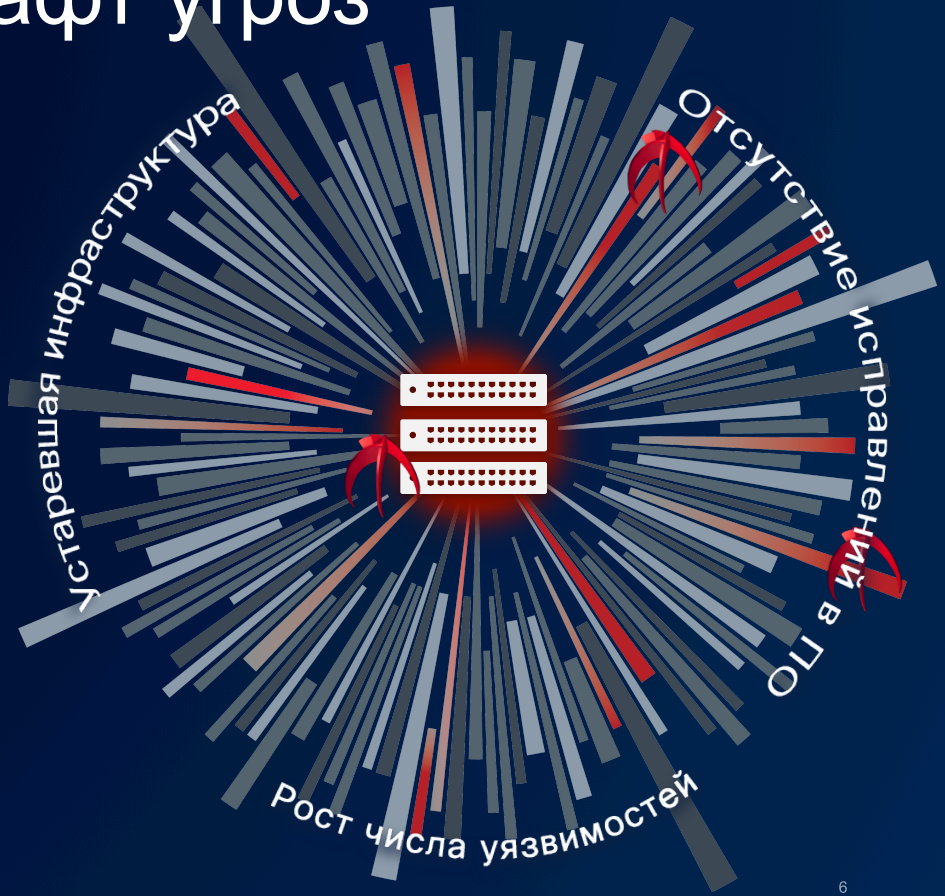
Увеличение запаса времени для преступных действий

Ускоренное принятие мер по защите

Глобальное влияние, локальные последствия

Современный ландшафт угроз

- Эволюция программ-вымогателей
- Совершенствование методов конспирации вредоносного кода
- Слабая культура безопасности сети
- Противоречивая геополитическая обстановка



Не новая, но самая доходная угроза

Стечение обстоятельств – легкое и эффективное шифрование, популярность эксплойт-китов и фишинга, а также готовность жертв платить выкуп шантажистам

Интересные наблюдения

Выплата выкупа не гарантирует расшифровки и восстановления данных

При повторной атаке некоторые вымогатели уменьшают сумму выкупа – «скидка для постоянных клиентов»

Ошибки в вымогательском ПО могут привести к невозможности восстановления данных даже при выплате выкупа

При задержке выплаты выкупа его сумма может возрастать

Инновации программ-вымогателей

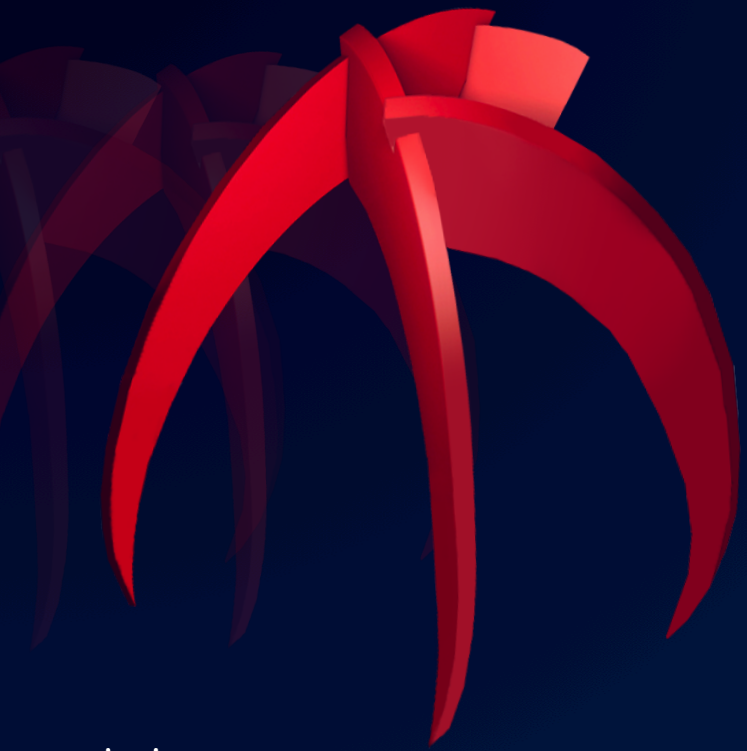
Индивидуальное шифрование для каждой цели

Использование биткойнов для анонимных платежей

Маркировка уже зашифрованных систем

Установка крайних сроков:
1. Для увеличения выкупа
2. Для удаления ключа шифрования

Программы-вымогатели второго поколения



Самораспространение

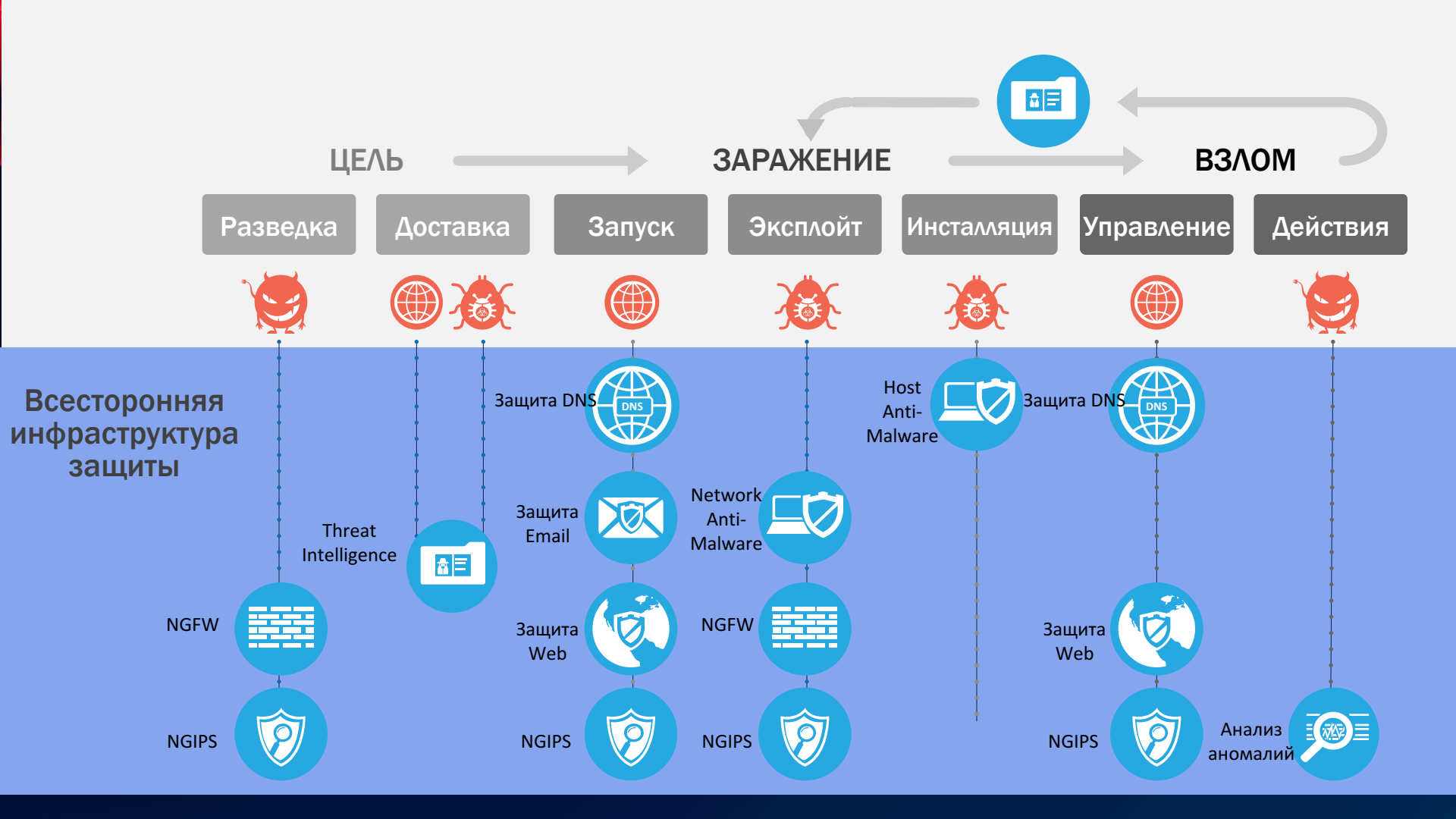
- Использование уязвимостей в широко распространенных продуктах
- Репликация на все доступные накопители
- Заражение файлов
- Базовые функции для атак методом подбора
- Устойчивость управления и контроля, в т.ч. полное отсутствие инфраструктуры контроля и управления
- Использование уже имеющегося в системе ВПО

Модульность

- Распространение через файлы автозапуска и USB-накопители большой емкости
- Эксплойты в инфраструктуре аутентификации
- Сложные системы управления, контроля и отчетности
- Ограничители потребления системных ресурсов
- Фильтрация целевых адресов для заражения (RFC 1918)

Какие протоколы используют вымогатели?

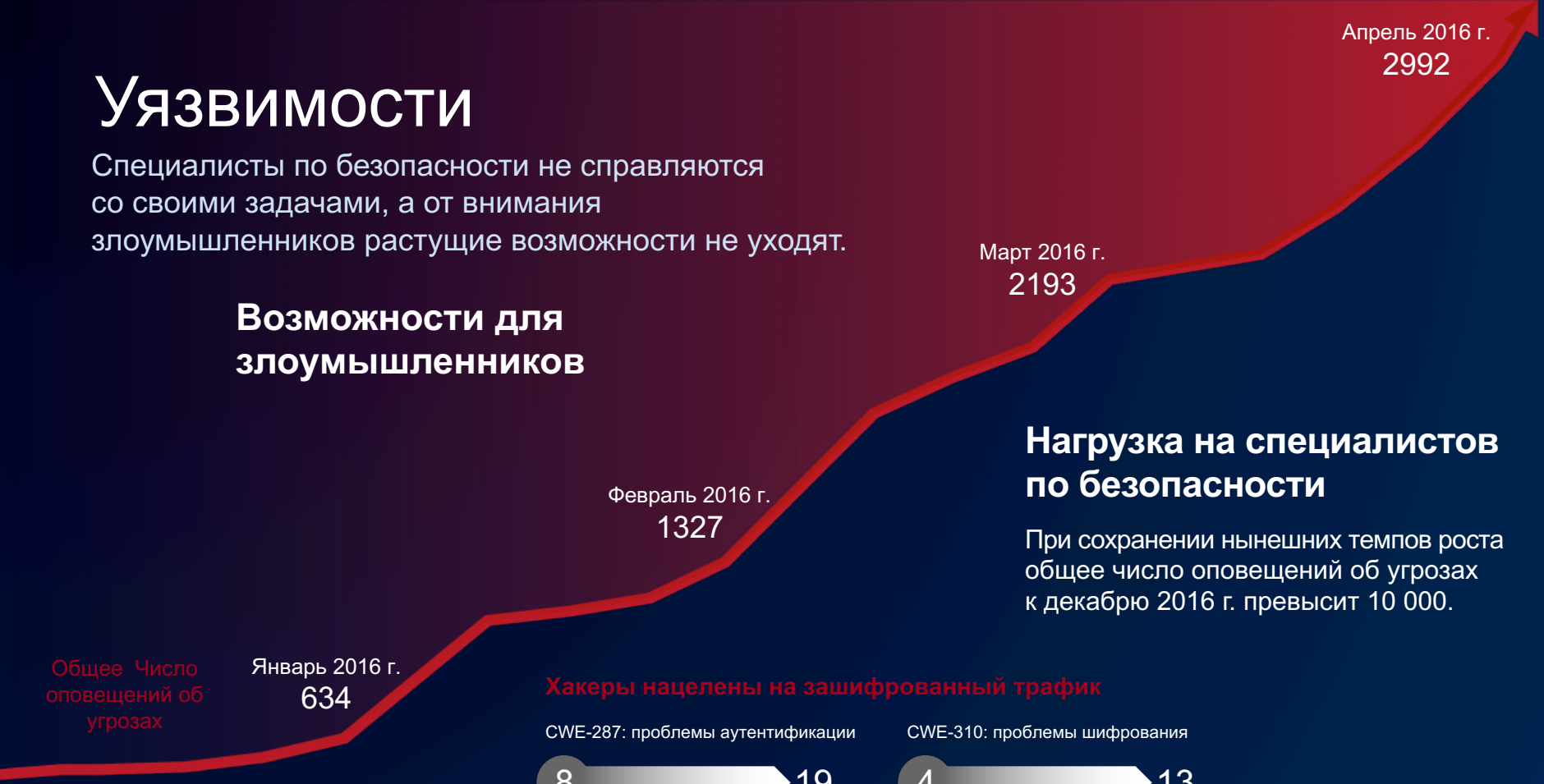
	Шифрование C&C				Шантаж
ИМЯ	**DNS**	**IP**	**NO C&C**	**TOR**	**ОПЛАТА**
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS


ЦЕЛЬ
ЗАРАЖЕНИЕ
ВЗЛОМ
Разведка
Доставка
Запуск
Эксплойт
Инсталляция
Управление
Действия
Всесторонняя инфраструктура защиты
Защита DNS
Host Anti-Malware
Защита DNS
Threat Intelligence
Защита Email
Network Anti-Malware
NGFW
Защита Web
NGFW
Защита Web
NGIPS
NGIPS
NGIPS
NGIPS
Анализ аномалий

Уязвимости

Специалисты по безопасности не справляются со своими задачами, а от внимания злоумышленников растущие возможности не уходят.

Возможности для злоумышленников



Нагрузка на специалистов по безопасности

При сохранении нынешних темпов роста общее число оповещений об угрозах к декабрю 2016 г. превысит 10 000.

Хакеры нацелены на зашифрованный трафик

CWE-287: проблемы аутентификации

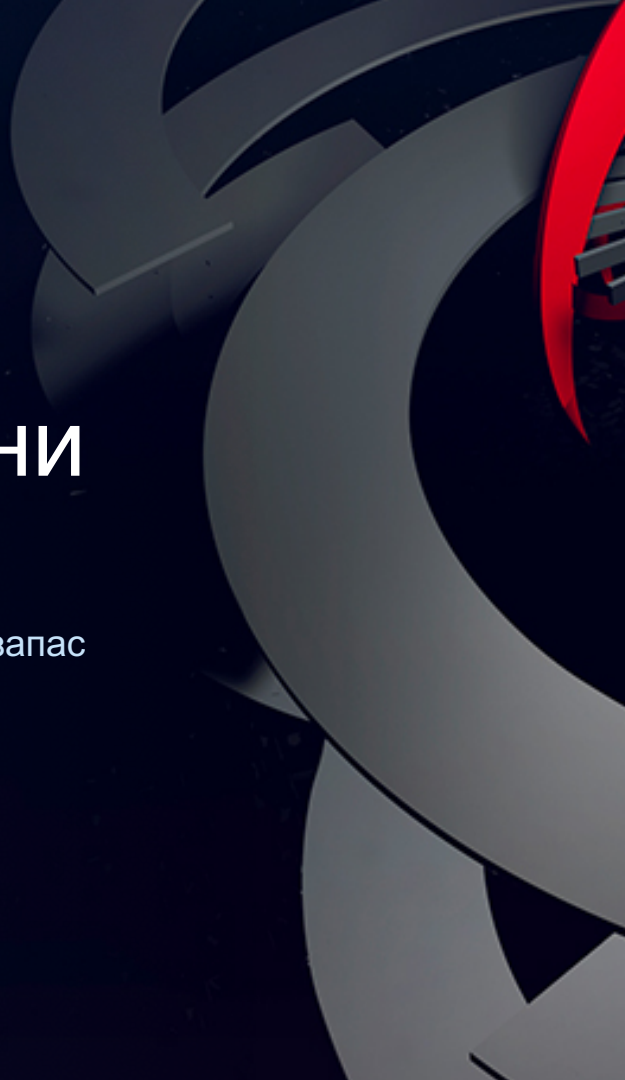
8 → 19

CWE-310: проблемы шифрования

4 → 13

Увеличение запаса времени для преступных действий

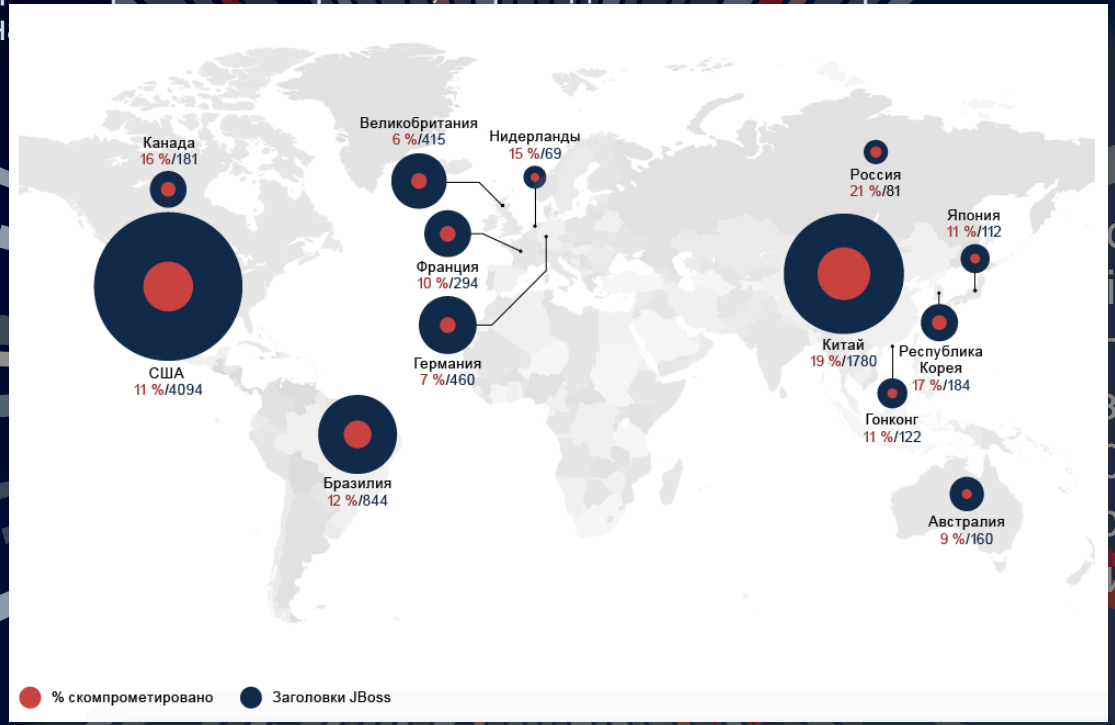
Злоумышленники не упускают выгоды, используя неограниченный запас времени для своих действий.



Векторы атак: на горизонте — серверы

Злоумышленники расширяют свои приемы, переходя от атак на стороне клиента к атакам н

Уязвимости в Adobe Flash до сих пор используются наборами эксплойтов.

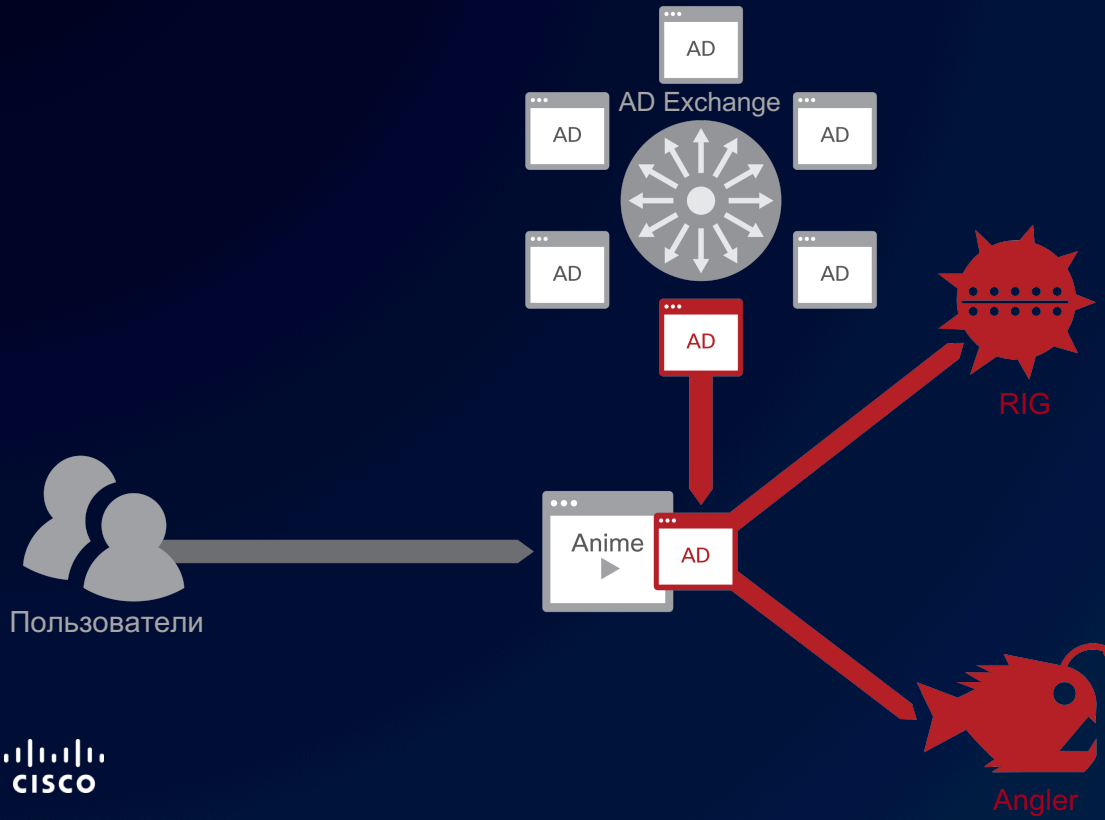


...о оценкам ...isco, в ...преле были ...зломаны ...0 % серверов ...oss по всему ...иру.

Комплекты эксплойтов: Adobe Flash и вредоносная реклама

Большинство наборов эксплойтов используют уязвимости Adobe Flash и Microsoft Silverlight

Вредоносная реклама как услуга: больше возможностей для дистрибьюторов



- Непосредственное заражение
- Переадресация на страницу с зараженными файлами
- Заражение в фоновом режиме
- Многократная переадресация

Использование HTTPS-трафика вредоносным ПО:

за последние четыре месяца объем HTTPS-трафика, используемого средствами вставки рекламы, вырос на 300 %

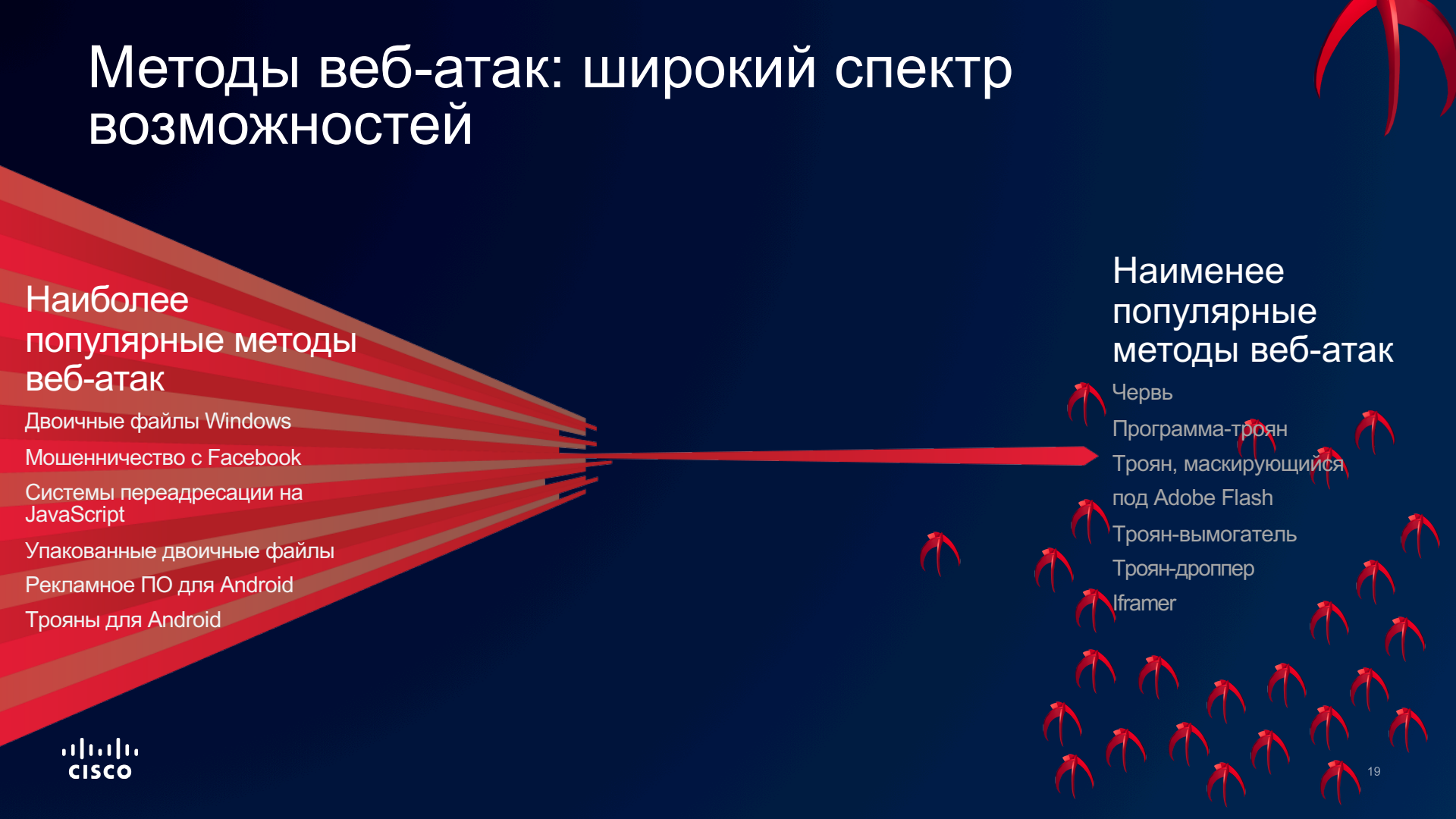
Увеличение на

300 %

за четыре месяца

Самая большая доля приходится на вставку рекламы (Ad Injector). Злоумышленники используют HTTPS-трафик, чтобы увеличить запас времени для своих действий.

Методы веб-атак: широкий спектр возможностей



Наиболее популярные методы веб-атак

Двоичные файлы Windows

Мошенничество с Facebook

Системы переадресации на JavaScript

Упакованные двоичные файлы

Рекламное ПО для Android

Трояны для Android

Наименее популярные методы веб-атак

Червь

Программа-троян

Троян, маскирующийся под Adobe Flash

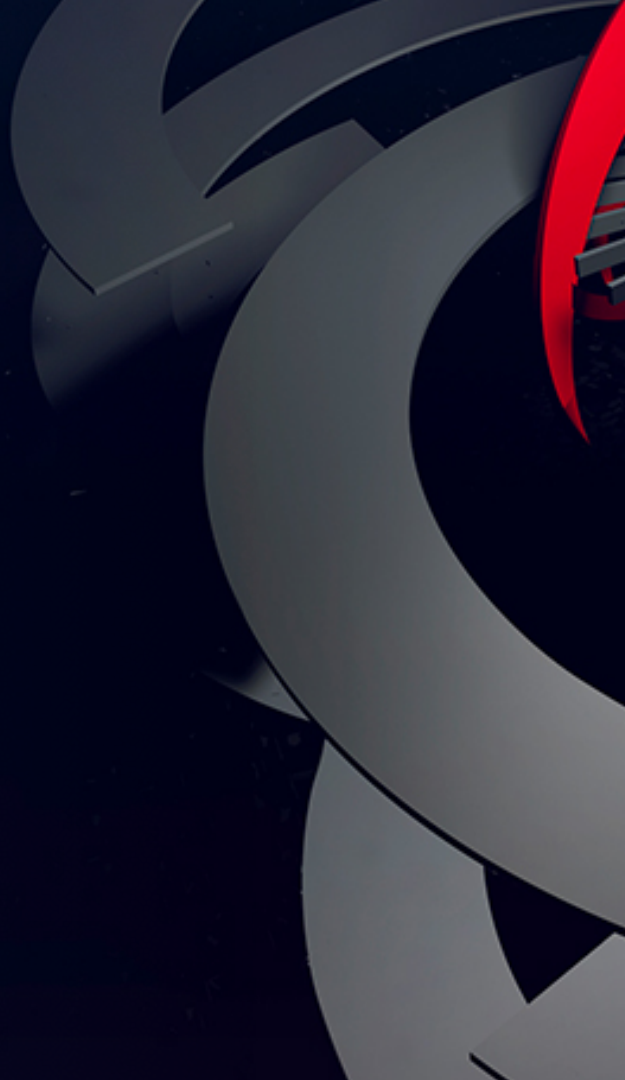
Троян-вымогатель

Троян-дроппер

Iframer

Ускоренное принятие мер по защите

Это лучший способ сорвать планы хакеров.



Время установки исправлений: автообновление и политика производителя

Браузеры
Chrome

Модель «Зубцы»

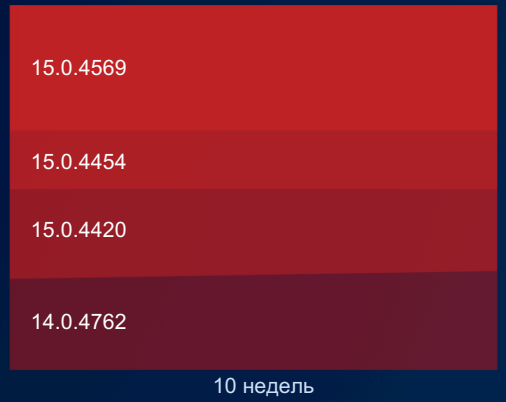
Обновления устанавливают пользователи, коэффициент внедрения высокий. Версии частично перекрывают друг друга.

Приложения
Java

Модель «Наклонные линии»

Обновления устанавливают и пользователи, и организации. Медленная миграция с огромным количеством различных версий, используемых одновременно.

Корпоративное ПО
Office



Модель «Прямоугольники»

Обновления устанавливают организации. Тенденция к обновлению версий очень слабая или вообще отсутствует. Уязвимости не устраняются.

Инфраструктура: создание цифровой экономики на базе уязвимой инфраструктуры

Слабая, уязвимая инфраструктура не сможет стать надежной опорой для экономики следующего поколения.

Устройства работают
с известными уязвимостями
в среднем

5 лет

И эта проблема носит системный характер

Cisco
5,64
лет

Apache/
OpenSSH
5,05
лет

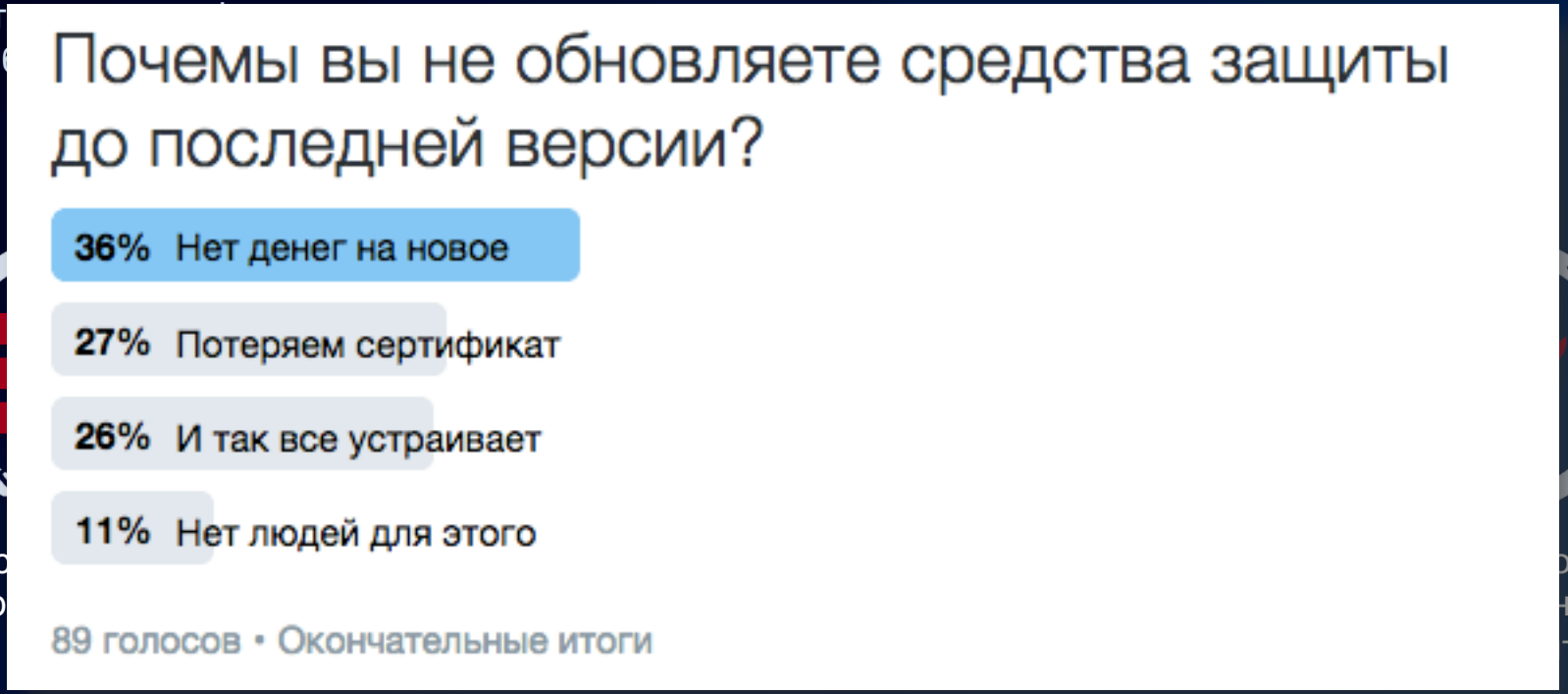
Устаревшая инфраструктура — общемировая проблема

Реагирование на инциденты: взгляд изнутри

Уст
по

Ус
инф

ован
ных
тов



Шифрование: заметая следы

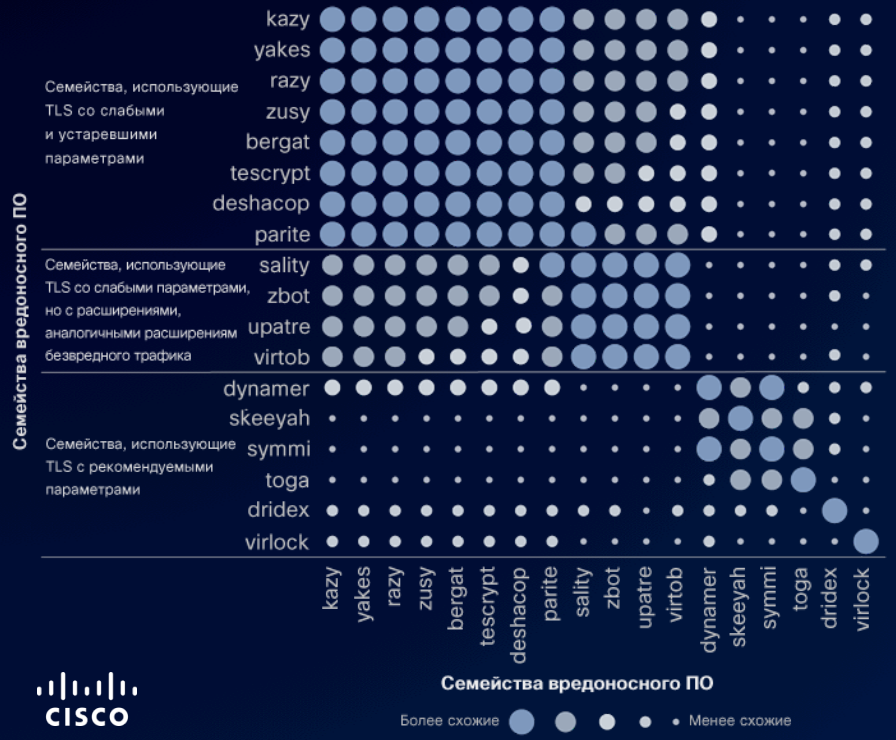
Злоумышленники скрывают свои следы в зашифрованном трафике, чтобы избежать обнаружения.

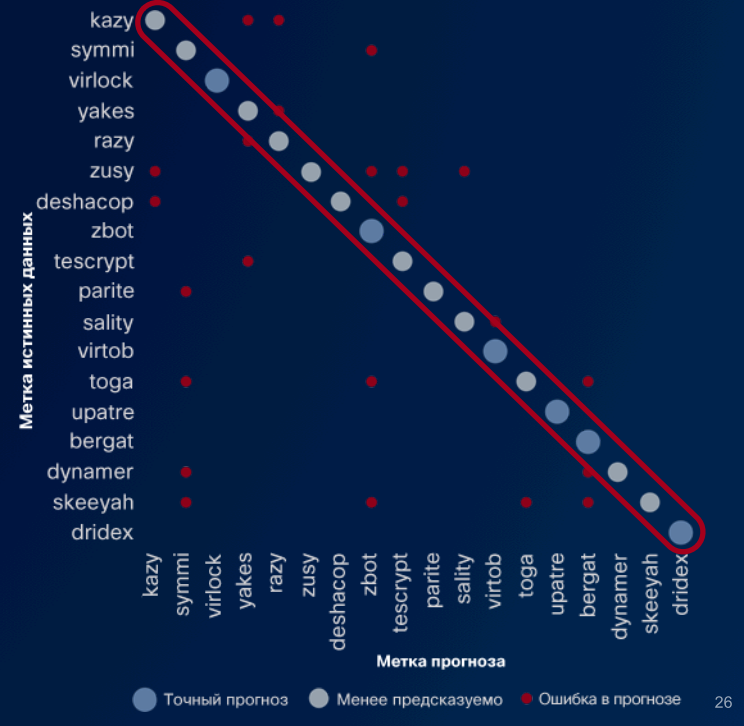
Увеличение вредоносного HTTP-трафика	Рост в %	Ср. % HTTPS
Рекламные объявления	+9,27 %	34,06 %
Поисковые системы и порталы	+8,58 %	64,27 %
Чат и мгновенный обмен сообщениями	+8,23 %	96,83 %

Категория, январь–апрель	Ср. % HTTPS
Корпоративная электронная почта	97,88 %
Чат и мгновенный обмен сообщениями	96,83 %
Веб-почта	96,31 %
Хранение и резервное копирование данных в режиме онлайн	95,70 %
Интернет-телефония	95,07 %

Использование TLS вредоносным ПО: обнаружение того, что нельзя обнаружить

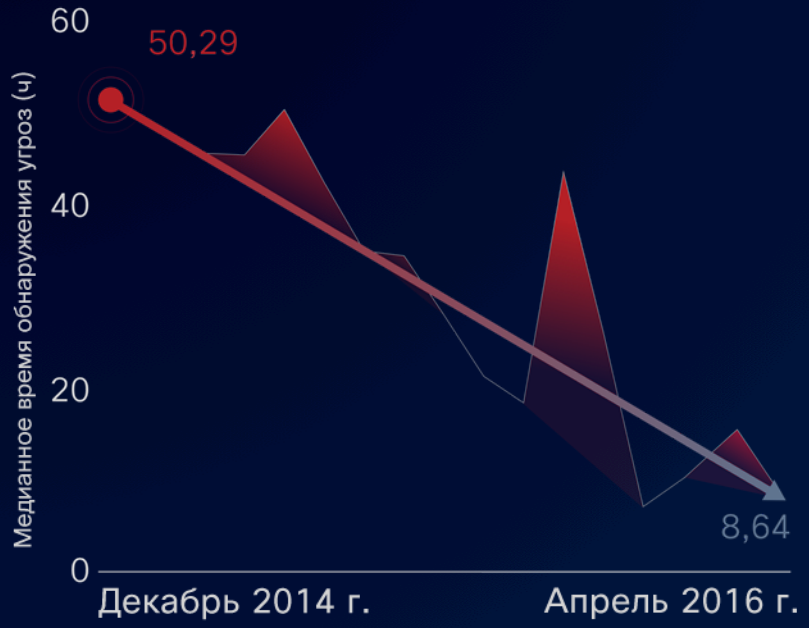
Благодаря машинному обучению можно точно обнаруживать и идентифицировать вредоносное ПО со сходными признаками.





Время обнаружения: более эффективное выявление злоумышленников

Получение преимущества в непрерывной «гонке вооружений».

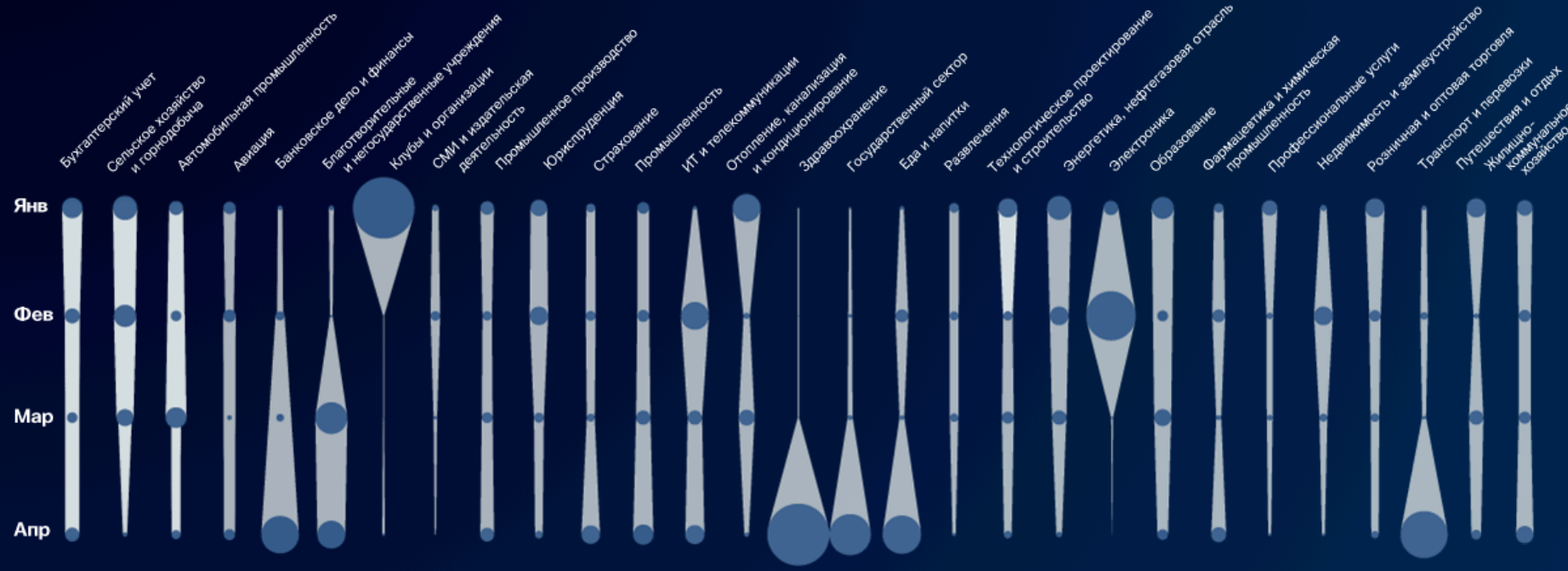


Глобальные перспективы

Хакеры действуют в глобальном масштабе, чтобы получить максимальную прибыль и избежать обнаружения.

Вертикальный риск борьбы с вредоносным ПО

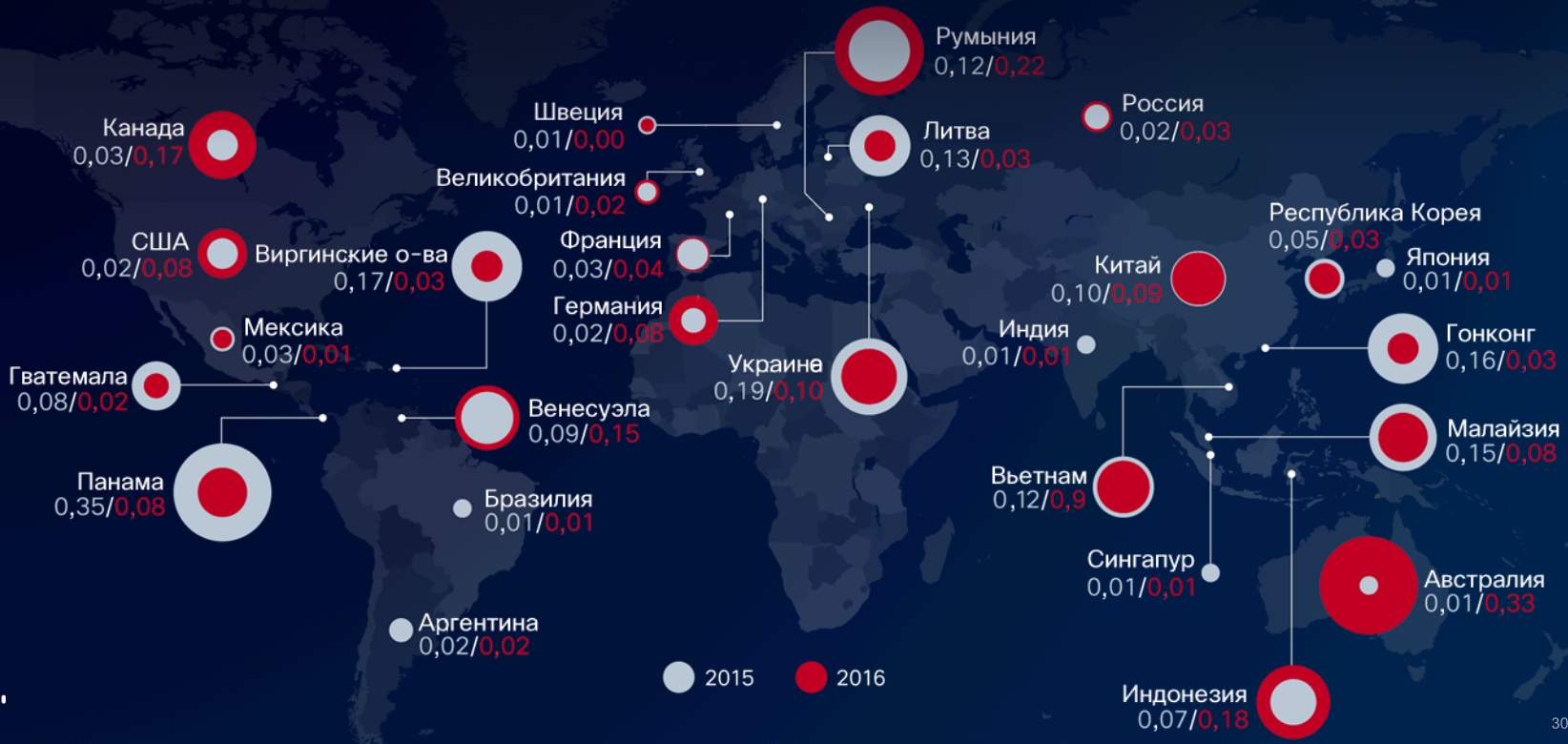
Все отрасли под угрозой. Хакеры переключаются с одной отрасли на другую.



Коэффициент возникновения угроз относительно базового показателя

Источники заблокированного веб-трафика по странам

Злоумышленники переносят базу своих действий из одного региона в другой, пренебрегая границами.



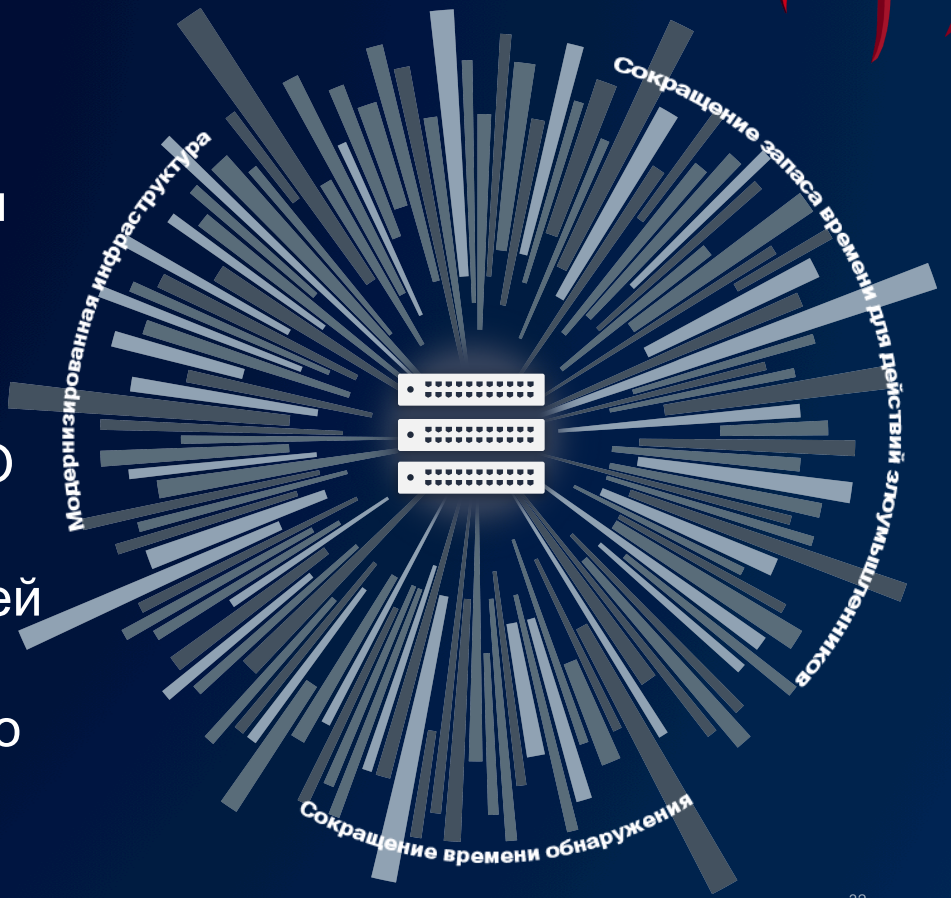
Геополитическая обстановка: противоречивые сигналы ограничивают информационную безопасность

Правительства стремятся установить собственные правила, но эти правила противоречивы

Общество также волнует проблема конфиденциальности

Выводы

- Выработать план реагирования (даже в случае успешной атаки вымогателя)
- Не доверять HTTPS/SSL/TLS
- Обновить инфраструктуру и ПО
- Провести повышение осведомленности пользователей по вопросам вымогателей
- Внедрить систему оперативного оповещения об угрозах



Отчет по кибербезопасности за первое полугодие 2016 г.

www.cisco.com/go/mcr2016

http://www.cisco.com/c/m/ru_ru/offers/sc04/2016-midyear-cybersecurity-report/index.html