

# ЭВОЛЮЦИЯ ВРЕДОНОСНОГО ПО

25 лет развития вредоносных программ

**1994**

**1**  
НОВЫЙ  
ВИРУС  
КАЖДЫЙ ЧАС



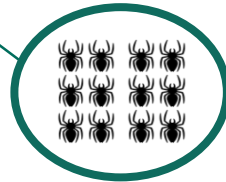
**2006**

**1**  
НОВЫЙ ВИРУС  
КАЖДУЮ  
МИНУТУ



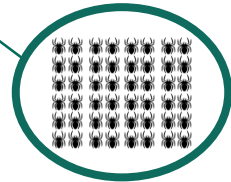
**2011**

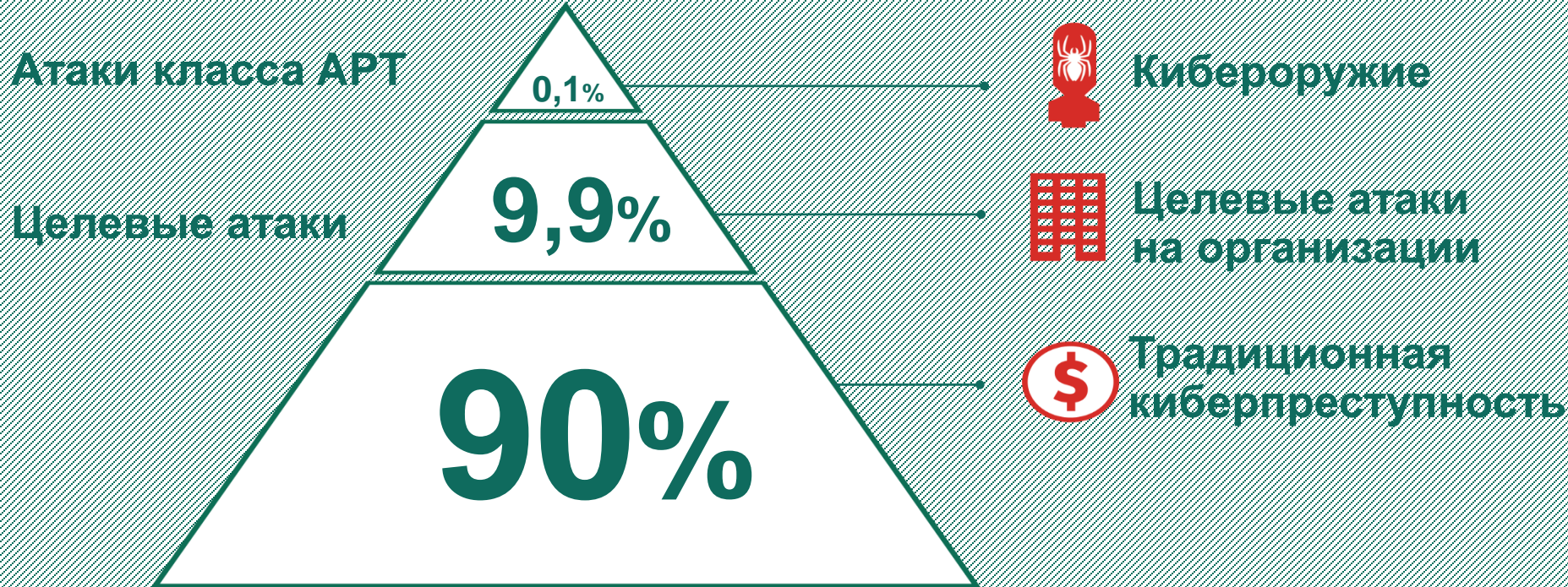
**1**  
НОВЫЙ ВИРУС  
КАЖДУЮ  
СЕКУНДУ



**2018**

**323 000**  
НОВЫХ  
ВРЕДНОСНЫХ  
ОБРАЗЦОВ В ДЕНЬ





# КАК РАСПРОСТРАНЯЕТСЯ ВРЕДНОСНОЕ ПО

Наборы  
эксплойтов



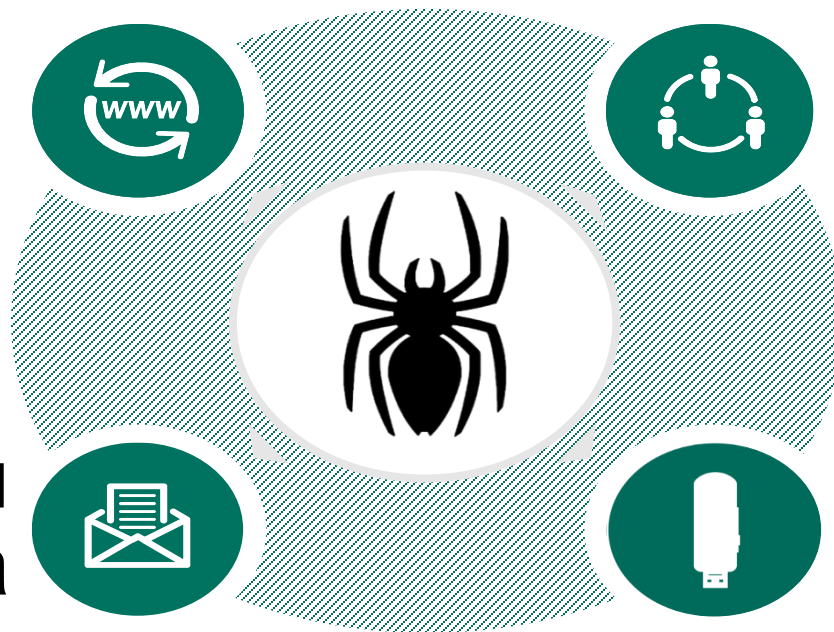
Социальные  
сети



Электронная  
почта



USB



Данные за:

2017

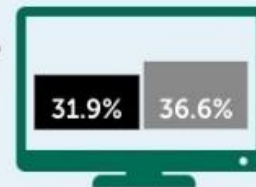
2016

## Интернет-угрозы

Число URL, признанных вредоносными



% пользователей, которые подверглись в интернете атакам вредоносного ПО хотя бы один раз за год



Число интернет-атак



Главные мишени интернет-атак с применением вредоносного ПО

1. Российская Федерация (42%) ↓
2. Казахстан (41%) ↓
3. Италия (39.9%) ↑

1. Казахстан (52%)
2. Российская Федерация (51.7%)
3. Украина (47.8%)

Источники интернет-атак

В 2017 году 78% атак было запущено с веб-ресурсов, расположенных всего в десяти странах мира

1. США (29.1%) ↑
2. Нидерланды (17%) ↑

1. США (24.1%)
2. Германия (13%)



## Банковские вредоносные программы

8 НОВЫХ

семейств вредоносного ПО для банковских и POS-терминалов



больше на 20% по сравнению с 2016



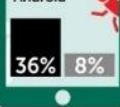
ТОП 3 стран-мишеней:

1. Российская Федерация
2. Бразилия
3. Турция



Svpeng, Gozi  
самые популярные банковские троянцы

увеличивается % атак на устройства Android



## Ransomware

62 новых семейства программ-вымогателей

С I по III квартал количество новых модификаций увеличилось

в 11 раз



ТОП 3

стран, атакованных шифровальщиками:

1. Япония
2. Италия
3. Хорватия



ТОП 3

программ-шифровальщиков:

1. CTB-Locker
2. Locky
3. TeslaCrypt

# ЭВОЛЮЦИЯ КИБЕРУГРОЗ В Q2 2018 ГОДА

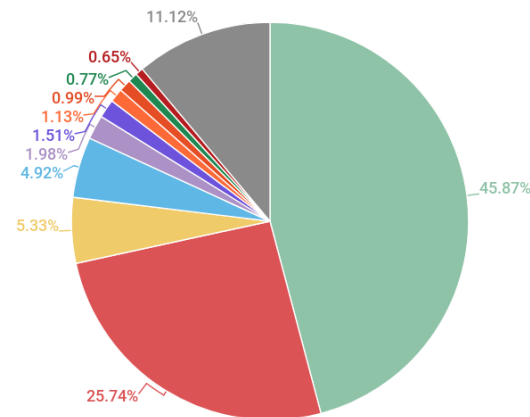
Основные цифры и статистика

## ОСНОВНАЯ СТАТИСТИКА: Q2 2018

- Решения «Лаборатории Касперского» отразили **962 947 023** атак, организованных с онлайн-ресурсов из разных стран мира
- Компоненты сетевой защиты признали вредоносными **351 913 075** уникальных URL
- Решения «Лаборатории Касперского» заблокировали попытки запуска вредоносного ПО для кражи денег через системы онлайн-банкинга на **215 762** устройствах
- Продукты «Лаборатории Касперского» заблокировали атаки программ-шифровальщиков на **240 799** устройствах
- Решения «Лаборатории Касперского» для защиты мобильных устройств обнаружили:
  - **1 744 244** вредоносных установочных пакетов
  - **61 045** банковских троянцев
  - **14 119** троянцев-вымогателей

## ГЕОГРАФИЯ ИСТОЧНИКОВ ВЕБ-АТАК: ТОП-10

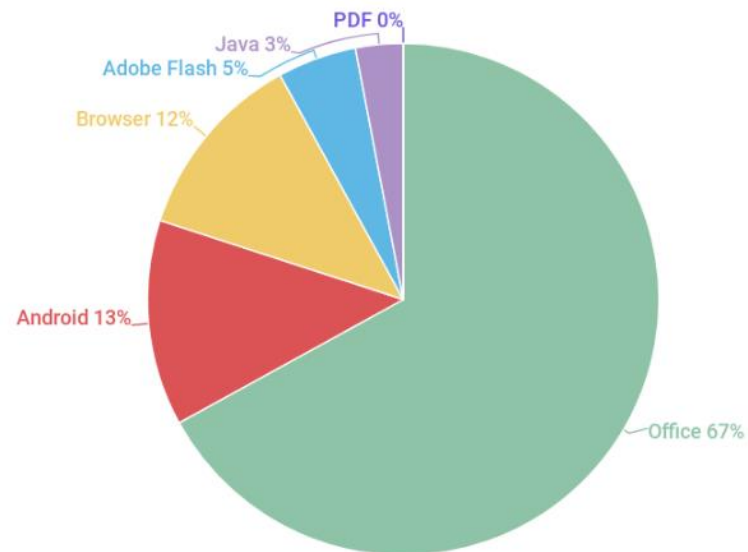
- Статистика основывается на физическом расположении ресурсов, которые использовались в атаках и были заблокированы антивирусными компонентами «Лаборатории Касперского» во втором квартале 2018 года
- Решения «Лаборатории Касперского» заблокировали **962 947 023** атак, выполненных с онлайн-ресурсов, расположенных в 187 странах мира
- **91,44%** ресурсов, использовавшихся для распространения вредоносного ПО, находятся в 11 странах
- В топ-5 стран, на территории которых находятся зараженные ресурсы, вошли США (45,87%), Нидерланды (25,74%), Германия (5,33%), Франция (4,92%) и Россия (1,98%)



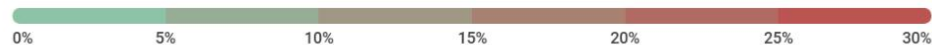
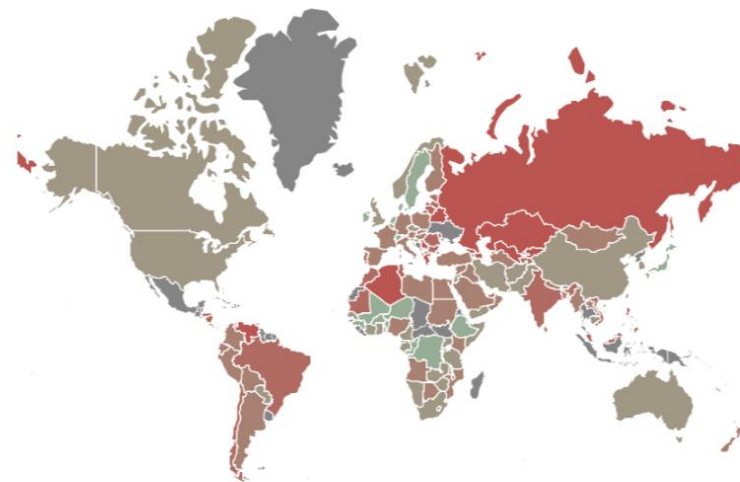


# УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ КИБЕРПРЕСТУПНИКАМИ

- Microsoft Office, Android, Браузеры, Adobe Flash Player и Java стали самыми уязвимыми приложениями во втором квартале 2018 года
- На долю браузеров пришлось **43,70%** всех эксплойтов
- Доля эксплойтов под приложения Microsoft Office (67%) увеличилась в два раза по сравнению с первым кварталом 2018 года (по сравнению со средним показателем за 2017 год — в четыре раза).
- Также во втором квартале мы наблюдали рост количества сетевых атак. Доля попыток эксплуатации уязвимостей, которые были исправлены в обновлении MS17-010, продолжает расти и составляет большую часть обнаруженных сетевых атак.

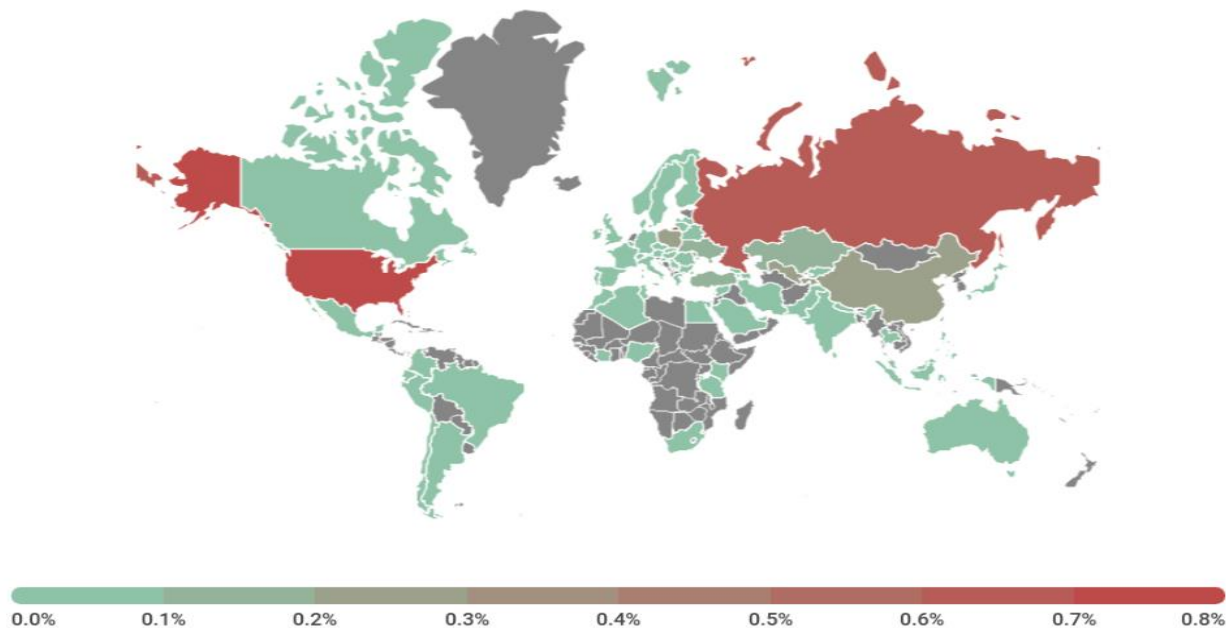


- В число стран с **ВЫСОКИМ РИСКОМ** онлайн заражения входят Белоруссия (33,49%), Албания (30,27%), Алжир (30,08%), Армения (29,98%), Украина (29,68%) и Молдова (29,49%)
- Среди **НАИБОЛЕЕ БЕЗОПАСНЫХ** стран Люксембург (14,4%), Германия (13,9%), Норвегия (13,83%), ЮАР (12,5%), США (10,56%), Уганда (10,29%) и Япония (9,18%)
- Во втором квартале 2018 года **19,59%** компьютеров подверглись по меньшей мере одной онлайн-атаке вредоносного ПО.



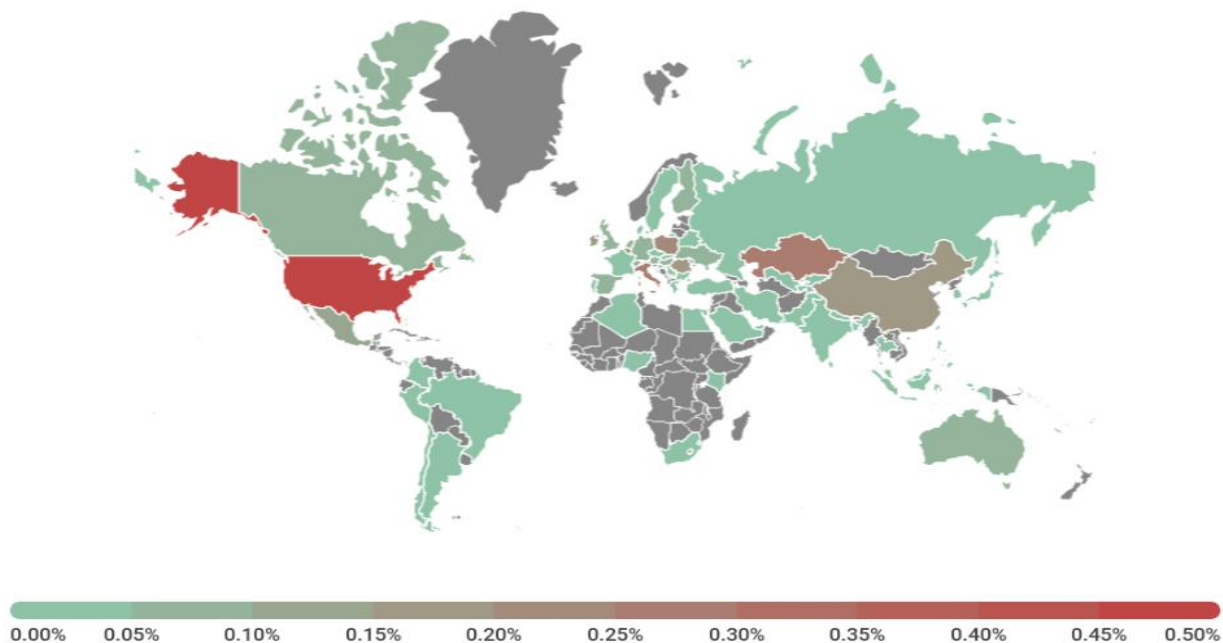
# ОНЛАЙН-УГРОЗЫ В БАНКОВСКОМ СЕКТОРЕ

- Во втором квартале 2018 года решения «Лаборатории Касперского» заблокировали попытки запуска вредоносного ПО для кражи денег через системы онлайн-банкинга на **61 045** устройствах.



## ПРОГРАММЫ-ВЫМОГАТЕЛИ

- Во втором квартале 2018 года решения «Лаборатории Касперского» заблокировали попытки шифрования данных вредоносными программами на **14 119** устройствах.



# ПРОГНОЗЫ НА 2019 ГОД

Что нас ждет в будущем?

## БУДУЩИЕ ПЕРСПЕКТИВЫ

- Индивидуальные импланты для каждой жертвы
  - Снижение пользы IoCs – индикаторов компрометации
- Исчезающее вредоносное ПО
  - Существует только в памяти и удаляется после перезагрузки
- Вредоносное ПО и международная политика
  - Дезориентация, манипуляция, слив данных, хакеры-активисты
- Киберсаботаж критической инфраструктуры
- Взлом Интернета вещей
  - Демонстрация уязвимости IoT девайсов
- Распространение модели «зловред как услуга» в финансовых атаках и атаках вымогателей
- Организаторы кампания кибершпионажа будут использовать социальные и рекламные сети
- Идентификация и выбор жертв

**СПАСИБО!**

**KASPERSKY**<sup>®</sup>