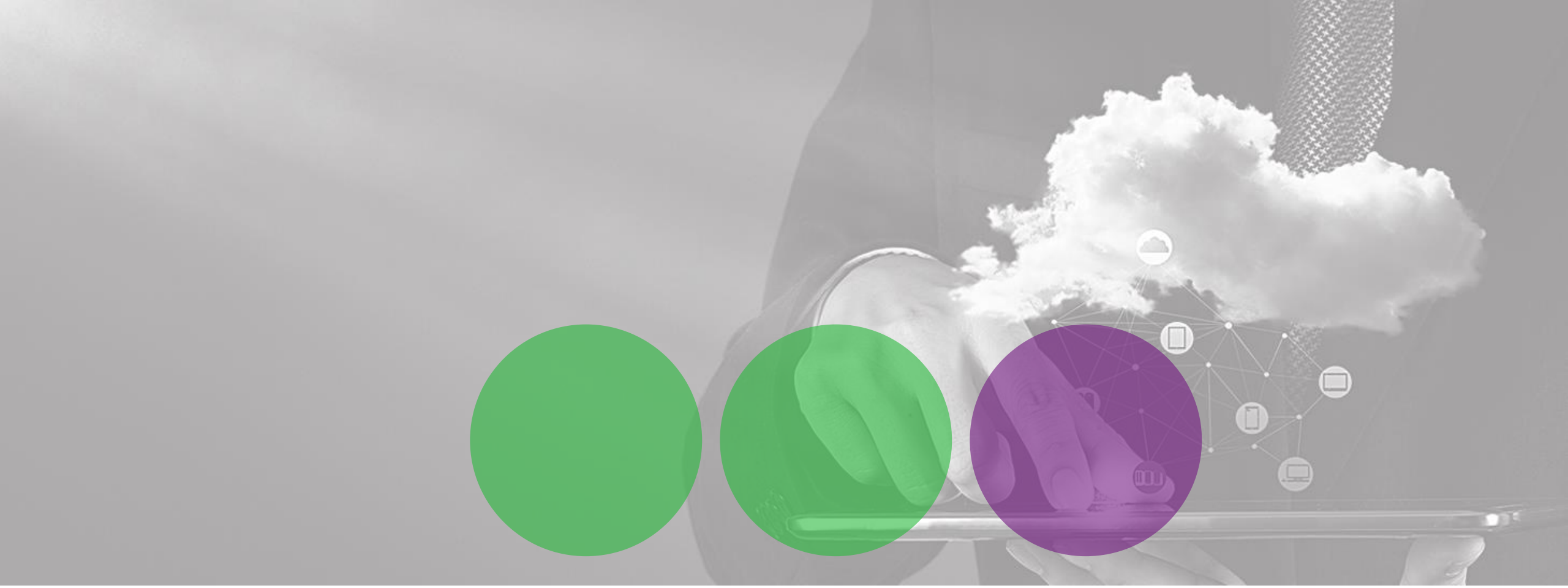
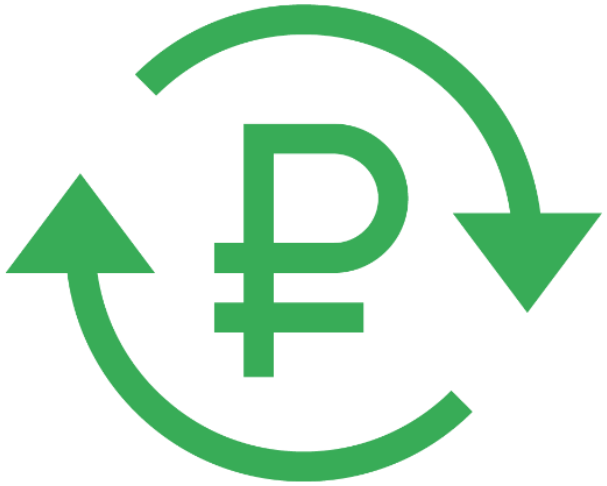


Услуги безопасности от телеком-оператора

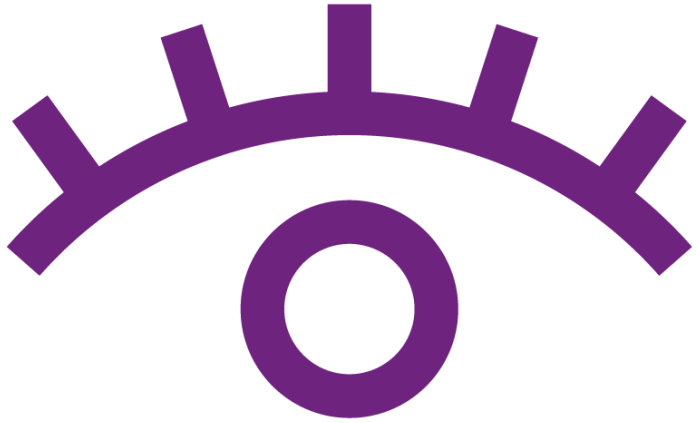
Виктор Азоркин, руководитель направления VAS-услуг в Уральском филиале

МегаФон

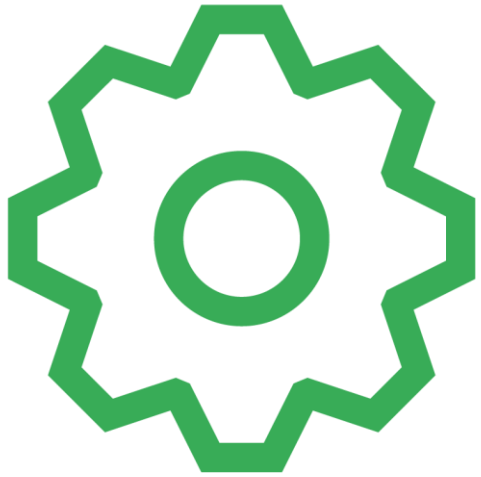
Предпосылки



Деньги



Информация



Маржинальность

Немного истории

Начало этого червя было предсказуемо и отслежено практически в реальном времени инженерами AT&T. Его можно было остановить до существенного замедления интернет-трафика.

- 2003 год
- SQL Slammer worm
- 75 000 хостов меньше чем за 10 минут

- Аномальный трафик по 1434 порту
- Window into the traffic

Новые возможности

Информация о трафике в реальном времени – бесценный ресурс

0 day ATTACK

Мы приближаемся к возможности спрофилировать и отразить сетевую атаку в момент ее зарождения

DDoS-атака

(от англ. Distributed Denial of Services - Распределенный отказ в обслуживании) – сетевая атака, заключающаяся в большом количестве одновременных запросов на сервера компании с целью доведения системы до отказа.

Успешная атака парализует работу сайта, пользователи не могут получить к нему доступ, либо он сильно затруднен. Это может привести к серьёзным финансовым и репутационным потерям, вымогательству, краже информации или шантажу.

DDoS-атака - одна из наиболее распространенных атак

В среднем в день мы отражаем 21 атаку*

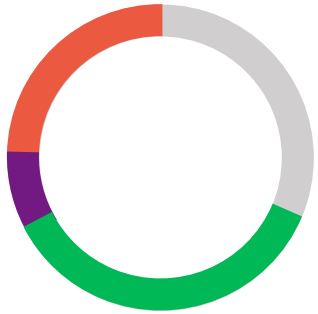
Сетевые атаки (3-4 уровень OSI)**

- В среднем за квартал ресурс атакуется 8,7 раз
- 67,4% целей атакуются повторно

Единичная атака	**36.7%**
2-5 атак	**38.2%**
6-9 атак	**12.4%**
10+ атак	**12.7%**

Атаки на приложения (7 уровень OSI)**

- **В среднем за квартал ресурс атакуется 8 раз**
- **63,3% целей атакуются повторно**



Единичная атака	**32.6%**
2-5 атак	**31.9%**
6-9 атак	**6.5%**
10+ атак	**29%**

МегаФон

* По статистике МегаФона

**Согласно отчету Imperva Incapsula «Global DDoS Threat Landscape Q4 2017»

Атаковать можно любую организацию

Наиболее частые цели:

Контент-провайдеры
и хостеры

СМИ

Интернет-магазины

Банки
и финансовые
порталы

Игровые сайты

Промышленные
организации

Интернет-ресурсы
государственных
органов

Образовательные
учреждения

МегаФон

Решение

Услуга «Защита от DDoS-атак» для клиентов, использующих «Доступ к сети Интернет» или «IP-транзит»

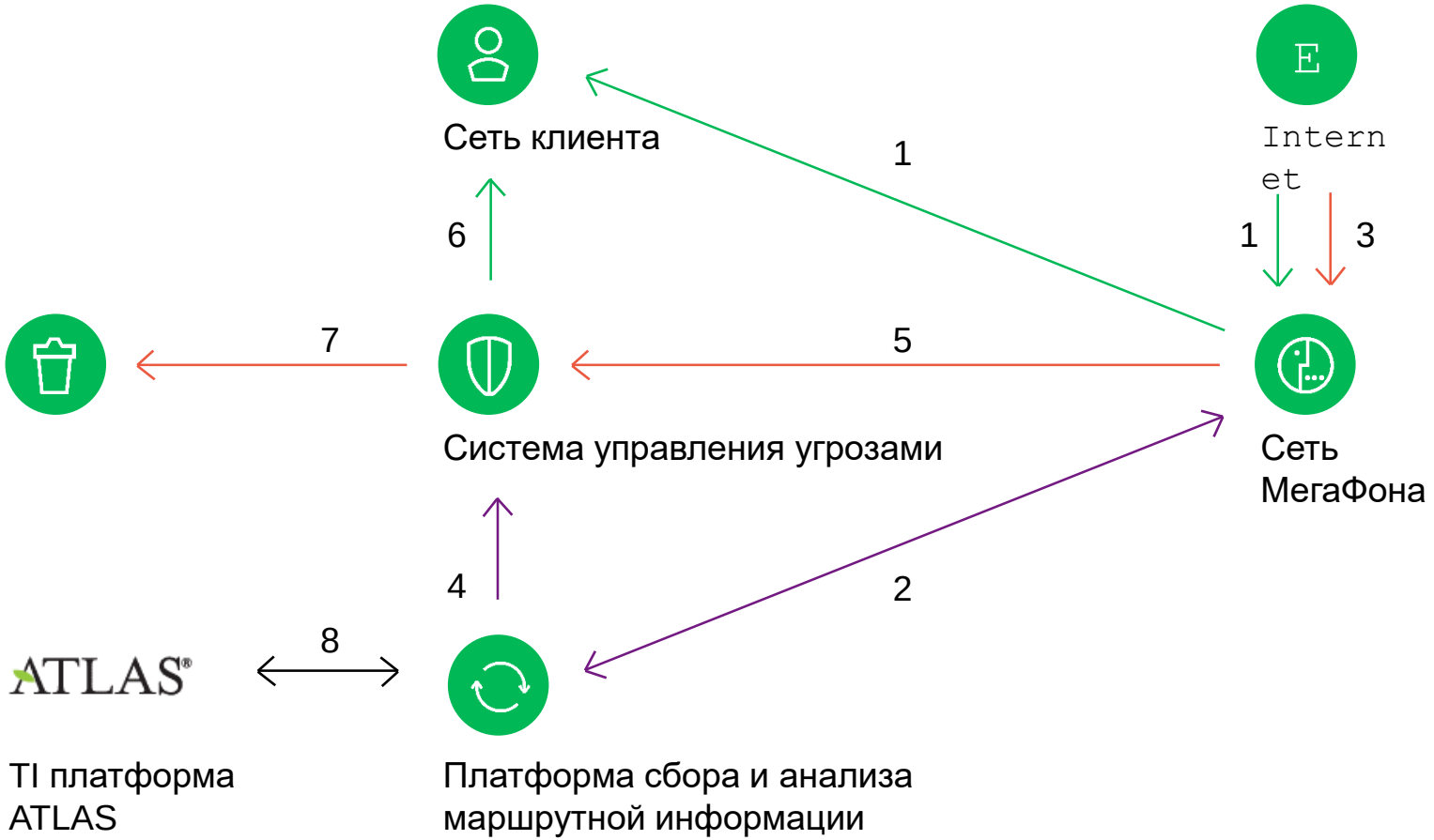
Решение построено на базе технологий Arbor Networks - мирового лидера по системам защиты от DDoS-атак

Защищает информационные ресурсы от перегрузок и DDoS-атак мощностью до 300 Гбит/с, не прерывая подключения обычных пользователей.

Обеспечит стабильную и бесперебойную работу интернет-ресурса при минимальных затратах

МегаФон

Как работает защита от DDoS-атак



1. Регулярный трафик
2. Постоянный анализ трафика
3. Трафик во время DDoS-атаки
4. Указание на фильтрацию трафика
5. Направление трафика на фильтрацию
6. Отфильтрованный трафик
7. Аннулирование вредоносного трафика
8. Обновление базы сигнатур

МегаФон

Технические преимущества

- Arbor Networks: Решение на базе лидера по системам защиты от DDoS-атак
- Отражение DDoS-атак мощностью до 300 Гбит/с на 3-7 уровнях модели OSI, включая атаки slow HTTP
- Автоматическое отслеживание и очистка трафика. Время включения фильтрации 5-15 секунд благодаря технологии Fast Flood Detection
- Возможность фильтрации шифрованного трафика (HTTPS) при установке оборудования в разрыв канала
- Три варианта технического обслуживания
- Ежедневное обновление базы угроз системой ATLAS на основе мировой статистики DDoS
- Не замедляет работу ресурса

МегаФон

От чего защитит

Volumetric Attacks – атаки, перегружающие каналы или оборудование для препятствования работе сервиса. Уровни OSI 3-4

Flood Attacks – атаки, переполняющие каналы связи за счет отправки большого числа запросов, не приводящих к установке соединения и создающих очередь "полуоткрытых соединений". Сервер перестает отвечать, а создание новых подключений невозможно

Application Layer Attacks – атаки на приложения (веб-сервера, сервера баз данных, VoIP телефонию и т.д.). Уровень OSI 7

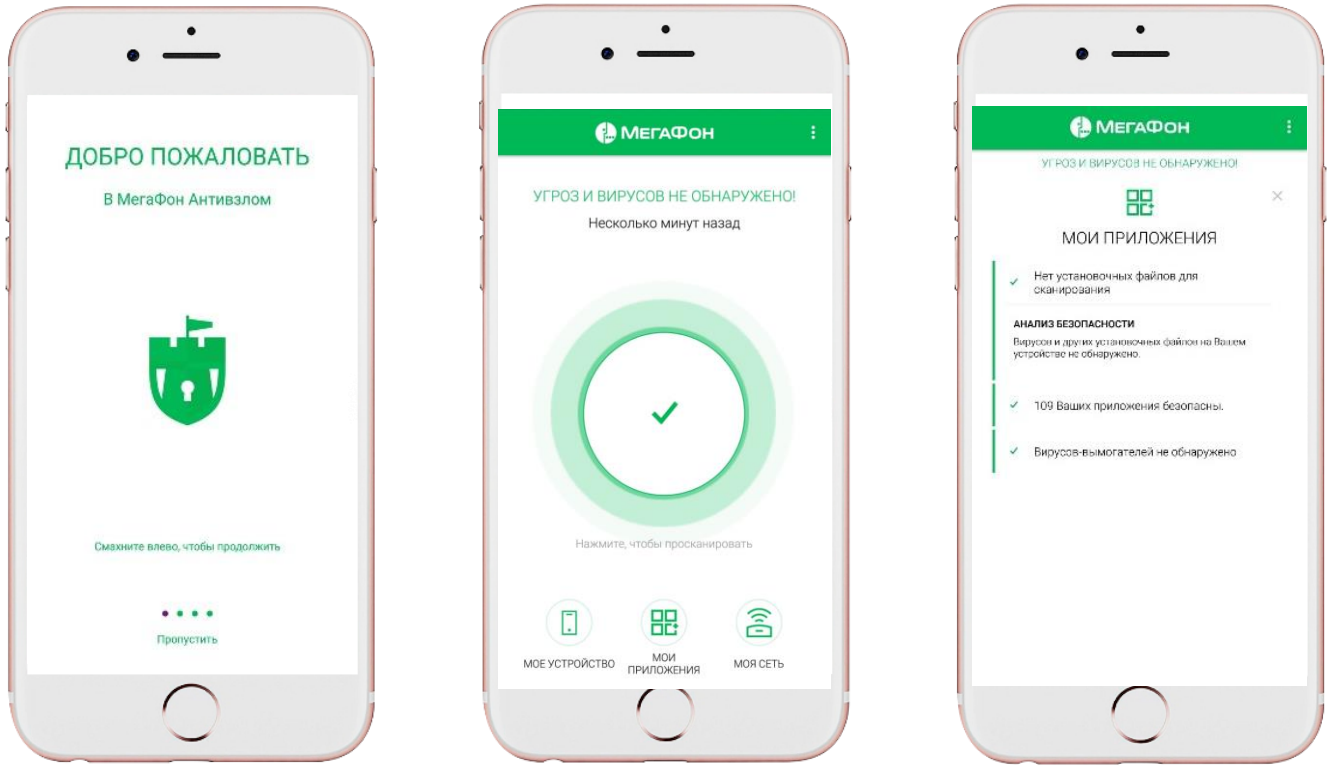
Amplification Attacks – атаки с использованием эффекта усиления (амплификатора) для увеличения мощности. Сравнительно небольшие ресурсы злоумышленника становятся причиной значительно большего ущерба или полного отказа работы системы-жертвы

«Медленные» атаки» – отправка большого числа запросов, передающихся с очень медленной скоростью, из-за чего ресурсы сервера используются гораздо дольше, препятствуя обработке запросов других пользователей

МегаФон

МегаФон Антивзлом

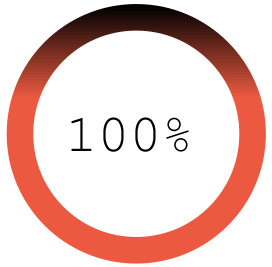
Решение для защиты мобильных устройств на базе Check Point SandBlast Mobile



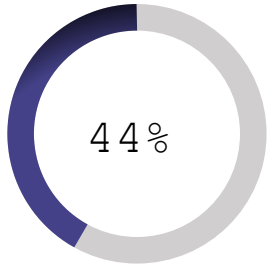
- Инновационный продукт на рынке
- Синергия с основным операторским бизнесом

Актуальность

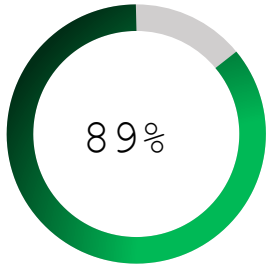
На мобильных устройствах хранится больше чувствительной информации, чем на ПК, но их легче взломать. Появляются новые мошеннические схемы, а антивирус больше не может обеспечить полную защиту. Мобильные атаки усложняются, а их число растет.



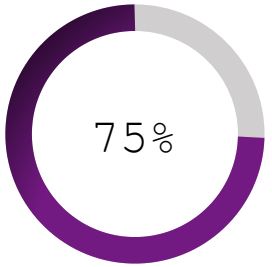
компаний хотя бы раз подверглись мобильной атаке в 2017 году. Возможно, они этого даже не заметили



всех троянских программ было обнаружено на устройствах сотрудников финансовой сферы



компаний подверглись хотя бы одной сетевой атаке через Wi-Fi



организаций имели хотя бы одно нелегитимно перепрошитое устройство с доступом в корпоративную сеть. Подобная перепрошивка (jailbreak / root) отключает встроенные защитные механизмы ОС

54 атаки

в среднем совершалось на одну организацию в 2017 году

1,6 млрд ₽

было похищено через мобильный банкинг с середины 2016 по середину 2017 года

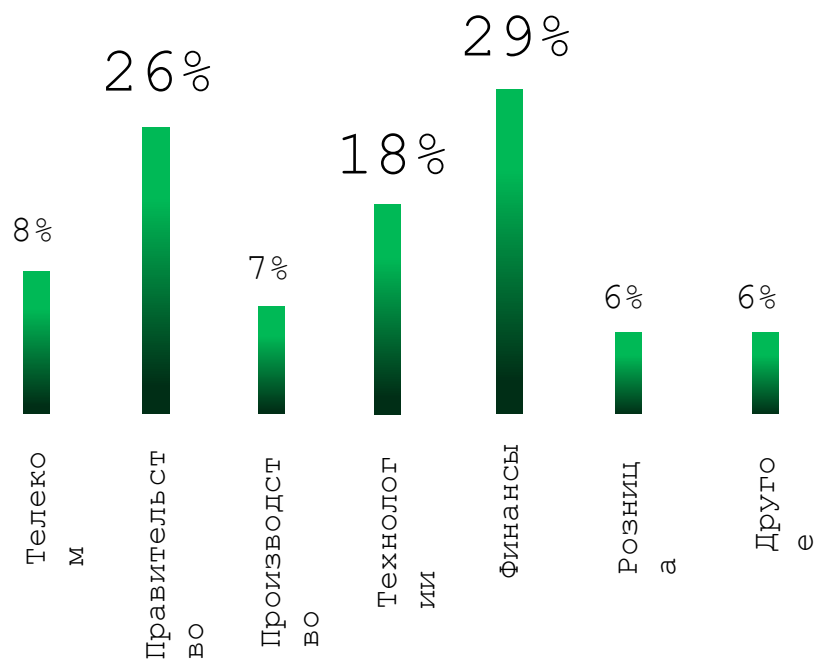
МегаФон

Данные представлены согласно отчётам Group-IB (2017), «A Check Point mobile threat research report» (2017) и «The Growing Threat of Mobile Device Security Breaches», Dimensional Research (2017).

Атаковать можно каждого

Большая часть атак приходится на Android, но iOS устройства также не защищены от взлома

Число атак по отраслям



Число атак на iOS по отраслям

МегаФон

Данные представлены согласно отчётам Group-IB (2017), «A Check Point mobile threat research report» (2017) и «The Growing Threat of Mobile Device Security Breaches», Dimensional Research (2017).

Основные типы мобильных атак

Перехват данных в Wi-Fi сети – при подключении к незащищённому или взломанному Wi-Fi трафик может быть перехвачен. Потенциально опасными являются общественные сети и другие сети без пароля. При подключении к такой сети пароли от банковских приложений и социальных сетей окажутся в руках мошенников за пару минут.

Вирус – вредоносное приложение, которое заражает устройство и мешает его работе.
Может замедлять или блокировать устройство, шифровать данные и доставлять прочие
неприятности. Защищаться от вирусов необходимо, но для полноценной защиты только
антивируса уже недостаточно.

Троянская программа (троян) – программа, которая отслеживает действия пользователя и передает их злоумышленнику. Получает доступ к датчикам на устройстве, таким как камера, микрофон и динамик.

Фишинг – атаки, в которых злоумышленник выманивает у жертвы логин и пароль. Например, создается копия известного пользователям сайта – банка, портала государственных услуг или рабочей почты. Ставка делается на невнимательность пользователя: он вводит свои данные, не проверяя адрес. Зачастую ссылки на такие сайты-двойники приходят на почту или в SMS.

МЕГАФОН

Давайте обсудим...

Виктор Азоркин
+7 922 222 7990
victor.azorkin@megafon.ru

МегаФон