Оценка рисков безопасности информационных систем

МегаФон

Кибербезопасность

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита
- Интернет под контролем (ИПК)
- Программно-аппаратный комплекс «Информационный периметр» (ПАК ИП)

Консалтинговые услуги и антифрод

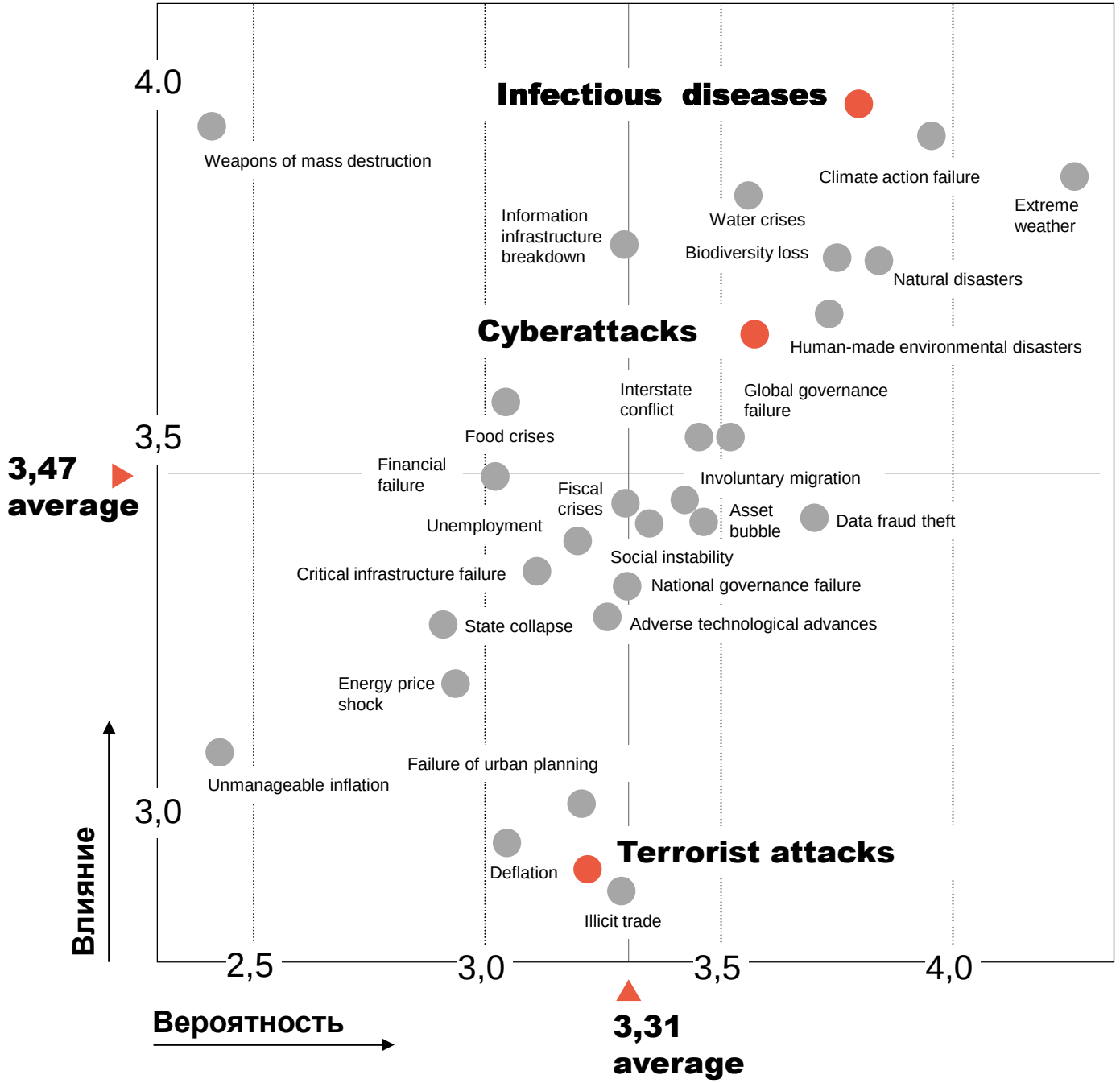
- Поиск уязвимостей Lite
- Threat Intelligence
- Анализ защищенности (Pentest)
- Antifraud
- Security Awareness

Защита данных

- Защита баз данных
- МегаФон DLP
- МегаФон EDR
- МегаФон MDM
- Антиспам,
- Антивзлом Бизнес

МегаФон

The Global Risks Report 2021



МЕГАФОН

Тестирование защищенности

Услуги

1. Тестирование на проникновение
2. Анализ защищенности
3. Аудит соответствия требованиям регуляторов и различных международных стандартов
4. Расследование инцидентов
5. Red teaming
6. Тестирование на устойчивость к Dos/DDoS-атакам
7. Удаленный офис (VPN, ВКС и т.д.)
8. Социальная инженерия (phishing)

Объекты тестирования

- Сети Wi-Fi
- Веб-приложения
- Мобильные приложения
- ДБО
- Бизнес приложения (ERP, CRM и т.д.)
- АБС
- Алгоритмы машинного обучения
- Блокчейн проекты
- Внешний периметр
- Внутренний периметр
- Сотрудники

МегаФон

Статистика

Корпоративная электронная почта — первоочередная цель для направленных вирусных и фишинговых атак, а также спам-рассылок

50 %
доля спама
в почтовом трафике

21 %
спама исходило
из России

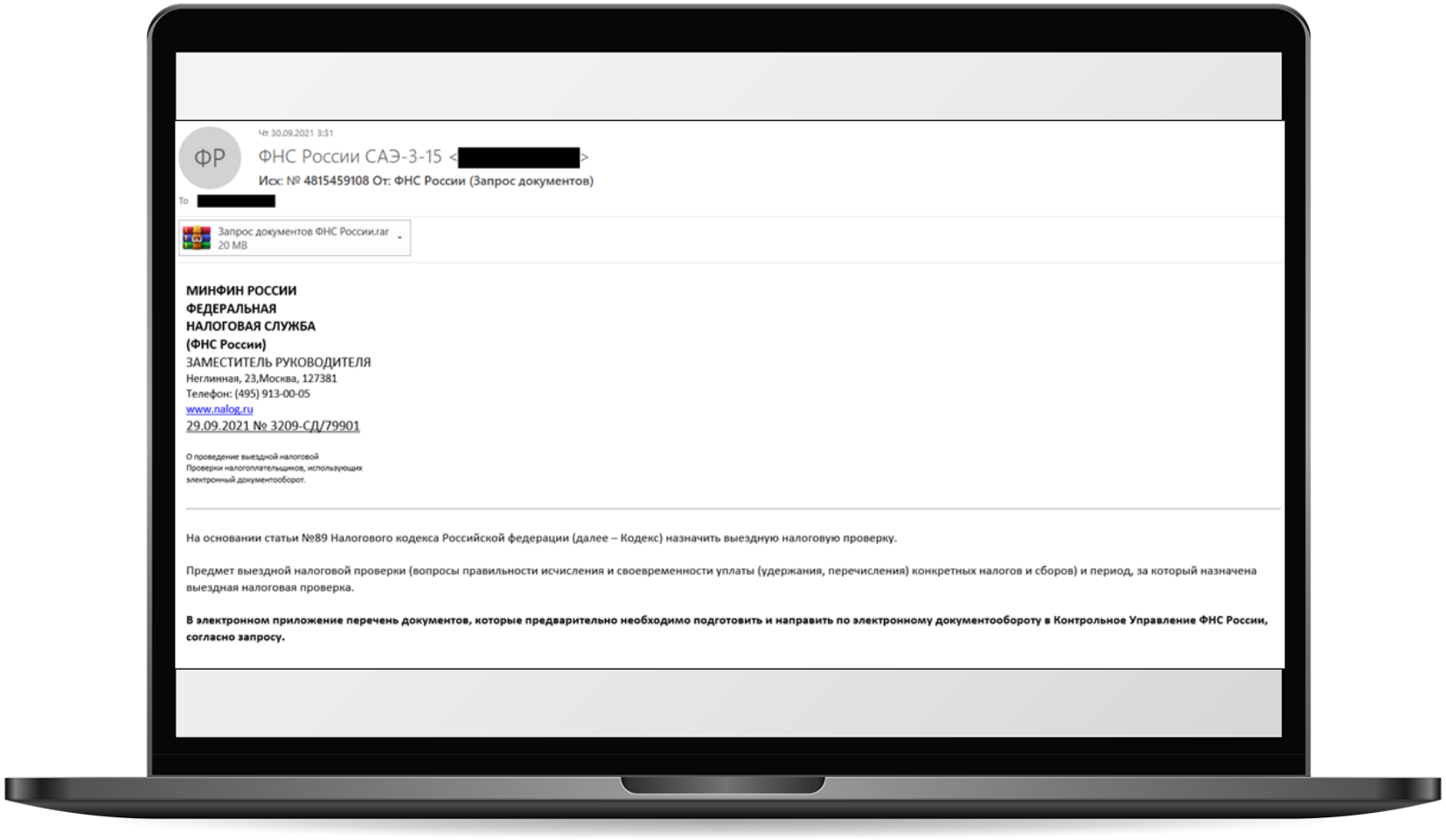
Чаще всего почтовый антивирус срабатывал на письма, содержащие «зловреды» этого семейства*

>184 млн
вредоносных вложений
обнаружено в письмах
в 2020 году

МегаФон

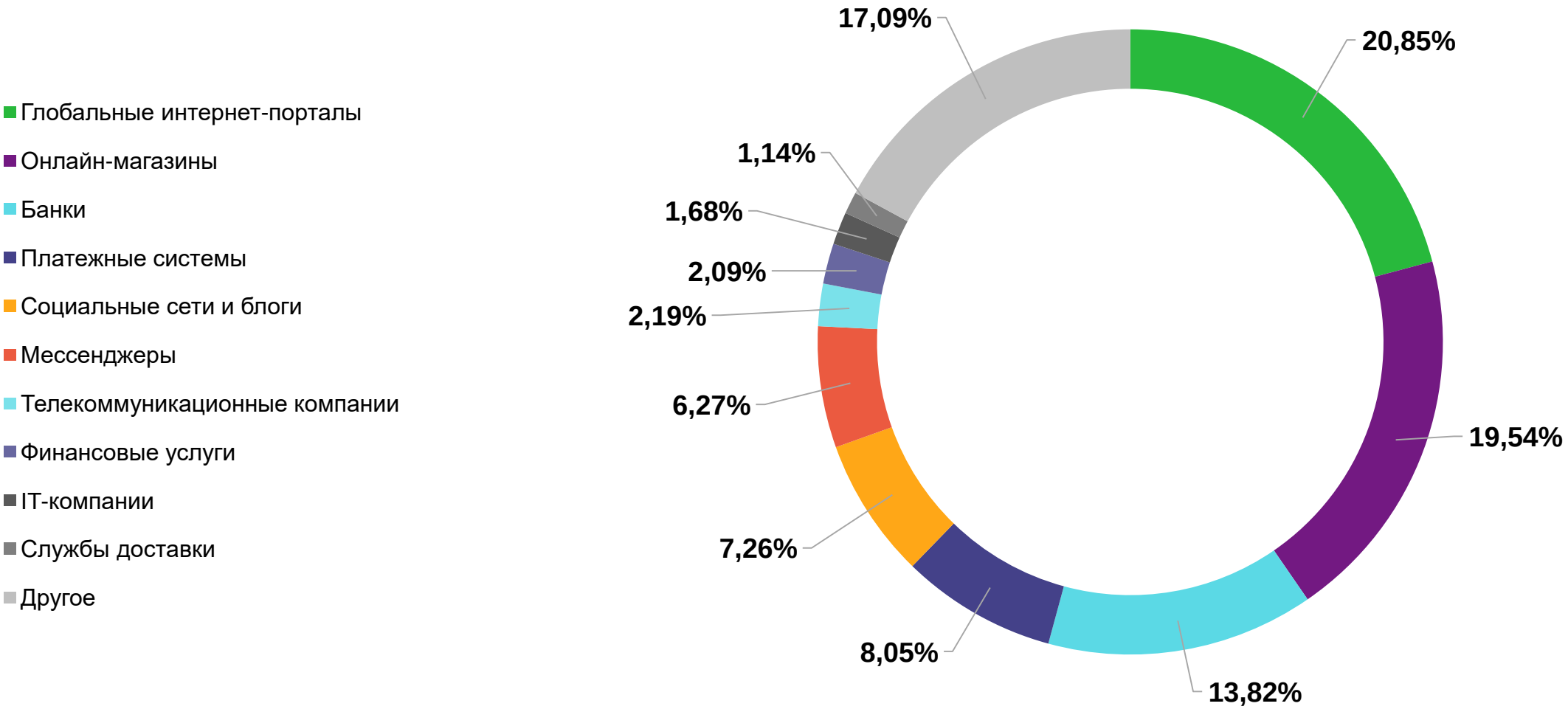
Источник: исследование Лаборатории Касперского, 2020
*Подробнее о Trojan.win32.agentb: Kaspersky Threats — Agentb

Примеры фишинга



МегаФон

Кто подвержен риску?



МегаФон

Источник: Отчет по спаму и фишингу за II квартал 2021 года | Securelist

Фишинг

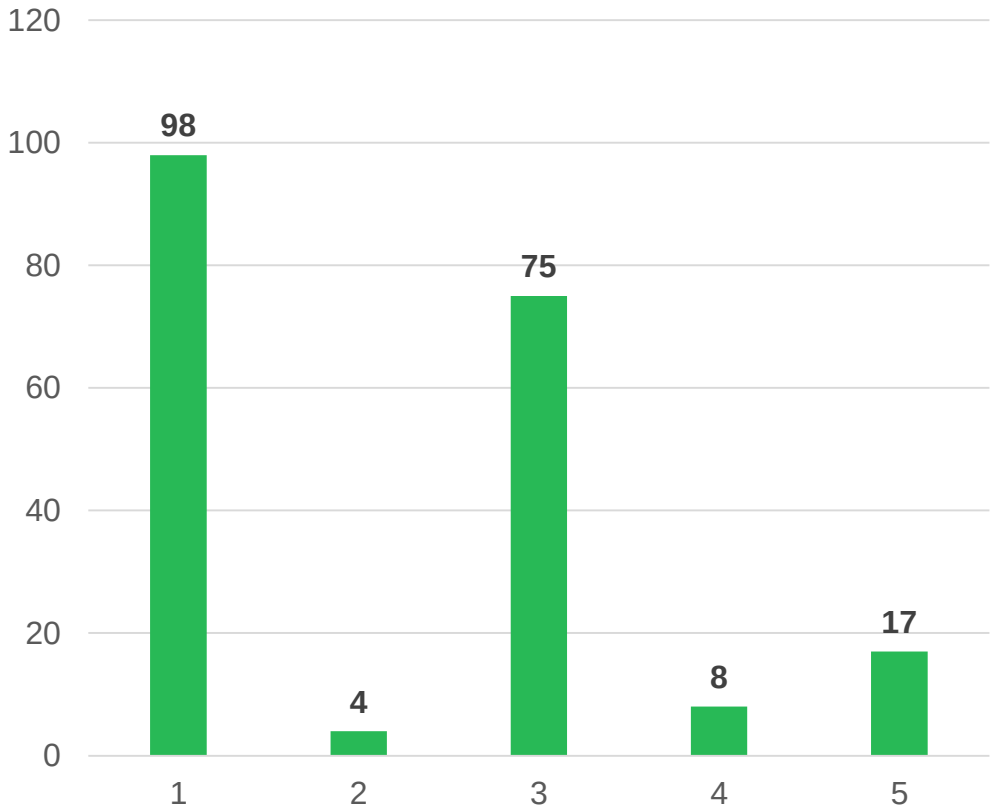
98 отправленных сообщений

Получено **4** ответных письма о проблемах с авторизацией

Собрано **75** учетных записей через портал

Максимально **8** попыток ввода учетных данных одним сотрудником

17 перехваченных хешей паролей



МегаФон

Примеры фишинга

МегаФон

МегаФон Security Awareness

Платформа содержит в себе материалы и набор теоретических блоков — всё необходимое для обучения базовым понятиям и правилам работы с информационными ресурсами

Встроенный в систему фишинговый модуль с множеством настроек. Фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

Гибкость и контроль

- Добавление собственных курсов
- Контроль процесса прохождения курсов
- Автоматизация процесса обучения при помощи гибкой системы

МегаФон

Наша команда

Закрытые уязвимости в GitHub, Mail.ru, Ozon, Qiwi, PayPal и т.д.

- Участники программ Bug Bounty
- Наличие сертификатов: CEH, CHFI, CND, MCSE, EXIN, OSCP, CISSP
- Опыт реализации различных кейсов в социальной инженерии
- Опыт расследования инцидентов ИБ
- Внедрение процессов SDLC
- Отбор на должность по реальному опыту
- Оперативная команда для выезда на инциденты
- Обучение правильному внедрению SDLC

МегаФон

Кибербезопасность

Сетевая безопасность

- Защита от DDoS
- WAF
- Криптозащита
- Интернет под контролем (ИПК)
- Программно-аппаратный комплекс «Информационный периметр» (ПАК ИП)

Консалтинговые услуги и антифрод

- Поиск уязвимостей Lite
- Threat Intelligence
- Анализ защищенности (Pentest)
- Antifraud
- Security Awareness

Защита данных

- **Защита баз данных**
- **МегаФон DLP**
- МегаФон EDR
- МегаФон MDM
- Антиспам
- Антивзлом Бизнес

МегаФон

Контакты

Мелёхин Артём
Руководитель по технологической поддержке
направления кибербезопасности

+7 926 167 31 78
artem.melekhin@megafon.ru

8 800 550 05 55
security.megafon.ru

МегаФон