RTM GROUP

Как взламывают финансовые организации?

Практика

Эксперт

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Евгений Царев

Управляющий RTM Group

Эксперт в области информационной безопасности и ИТ-права (более 15 лет профессионального опыта)

О компании RTM Group

RTM Group — ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права.

Работаем на всей территории России, Беларуси и Казахстана, и не ограничиваемся на этом. Головной офис компании находится в Москве, производственное подразделение базируется в Воронеже.

RTM Group ежегодно выполняет сотни проектов, делая свой вклад в стабильность и безопасность киберпространства, а также помогает провести анализ цифровых доказательств для судов и следственных органов.

90+

Проектов по построению комплексной системы информационной безопасности

70+

Судебных экспертиз, по фактам нарушения режима защиты информации проведены нашими экспертами

60+

Завершенных проектов по защите информации ограниченного доступа

30+

Судебных экспертиз, связанных с хищением денежных средств банков и их клиентов с использованием ДБО

RTM GROUP

Содержание

Внешние атаки на организацию

Внешние атаки на организацию:

Очень низкая доля успешности проникновения в КИС

менее **5%**

Банальные просчеты в реализации политик ИБ

в **90%** случаев

Высокая доля атак на отказ в обслуживании

более **75%**

***** все чаще фиксируем развитие многовекторных DDoS-атак**

Внутренние угрозы в финансовых компаниях

Причины:

Некорректное разграничение прав доступа	более **80%** успешных атак
Устаревшее/неподдерживаемое прикладное или системное ПО	более **60%** успешных атак
Отсутствие сегментации сети	более **50%** успешных атак
Нехватка основных средств защиты информации	более **90%** успешных атак
Некорректные конфигурации или архитектура DLP, SIEM, EDR, SOAR	• **100%** успешных атак
Человеческий фактор как источник «сливов» КИ	• в **99%** случаев

RTM GROUP

Социальная инженерия

Статистика атак посредством социальной инженерии и утечек конфиденциальной информации.

70%

Атак используют E-mail

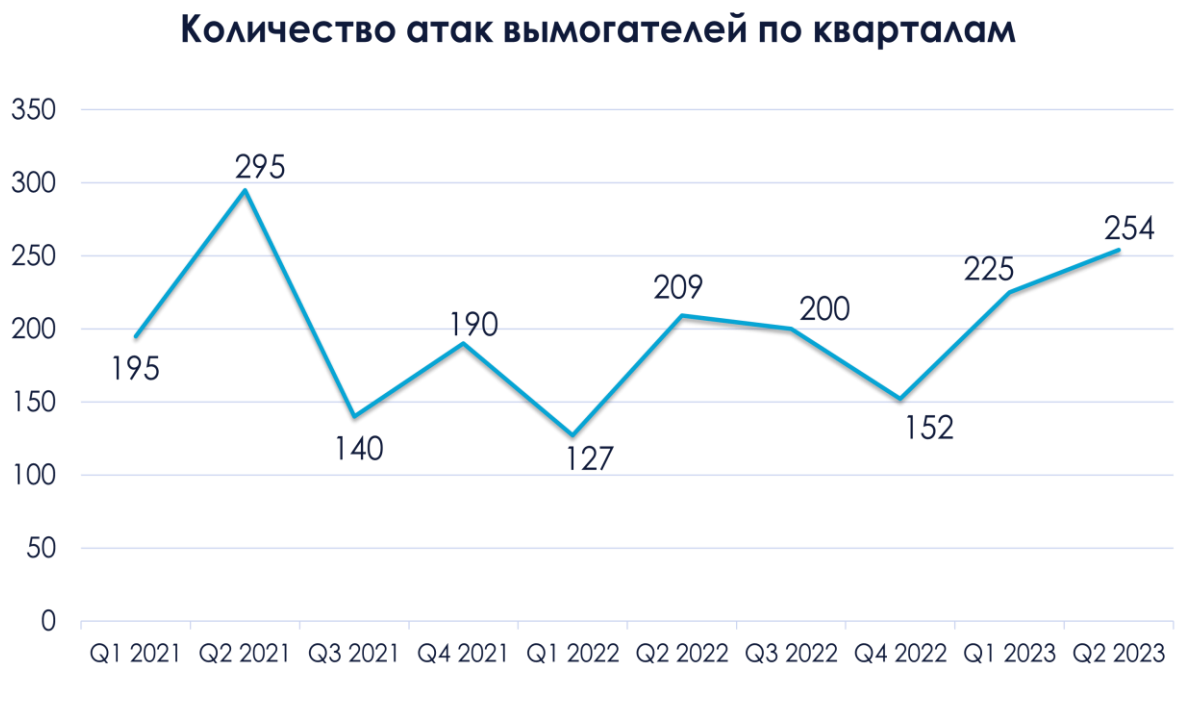
≈ 95%

Вероятность успеха при телефонном звонке

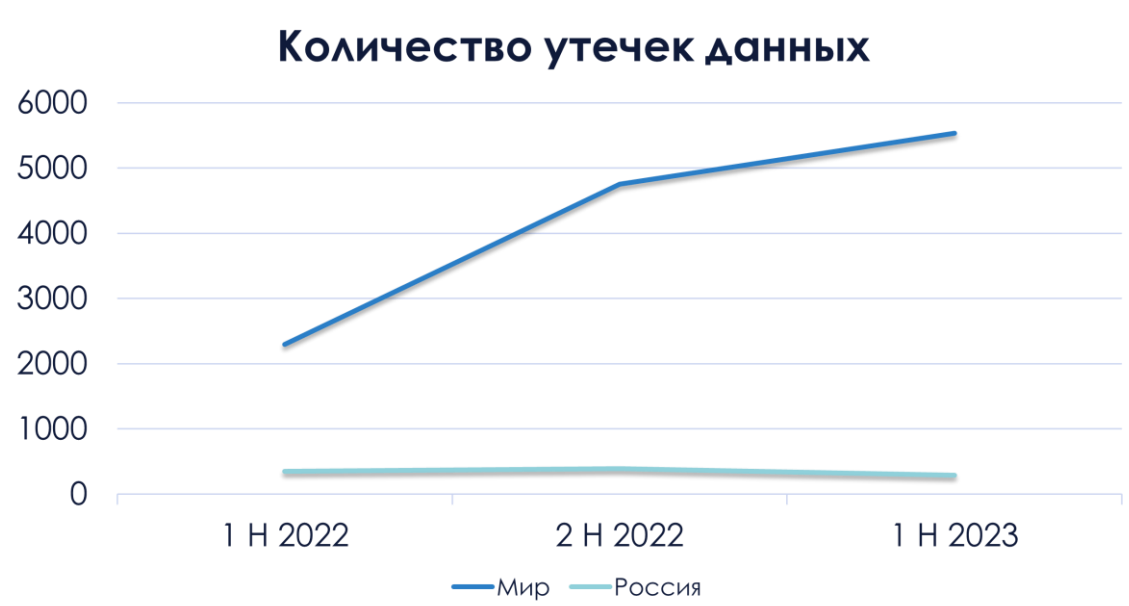
≈ 80%

Вероятность проникновения в контролируемую зону

Статистика социнженерии и утечек конфиденциальной информации



© Positive Technologies



© InfoWatch

RTM GROUP

Сценарии социотехнического тестирования

- С использованием e-mail (80% популярности, 20% эффективности)
- По телефону (5% популярности, 50% эффективности)
- При личной встрече (2% популярности, 70% эффективности)
- Методом разбрасывания зараженных носителей (менее 1% популярности, менее 1% эффективности)

Способы исправить ситуацию

RTM GROUP

Предотвращение атак — это процесс!

Планирование (не «для галочки»)

Документация

Реализация (в соответствии с планом)

Внедрение

Контроль (независимый)

Пентест и аудит

Совершенствование (регулярное)

Добрая воля

RTM GROUP

Telegram-канал

ИТ. Право. Безопасность

@it_law_security

Экспертный контент и срочные новости из мира ИБ

Спасибо за внимание!

Готовы ответить на Ваши вопросы


+7 (495) 197-64-95


info@rtmtech.ru


https://rtmtech.ru


@RTM_Group


rtm.group


it_law_security