Райффайзен БАНК

Что будет с фродом после ~~Covid~~ социнженерии

Противодействие киберфроду

Просто. Четко.
Компетентно.

Почему идет спад социнженерии?

AML и антифрод

Контроль движения средств работает как для предотвращения хищений, так и при легализации и обороте похищенных средств.

Всеобщая цифровизация финансовых отношений позволяет отследить цепочки и проявляет нехарактерные движения средств.

Работа операторов связи

Массовая блокировка подмен официальных номеров банков/организаций потребовала уход мошенников на случайные «незнакомые» номера.

Внедрение антифрод систем операторами с предоставлением сервисов для защиты от подмен номеров.

Иммунитет

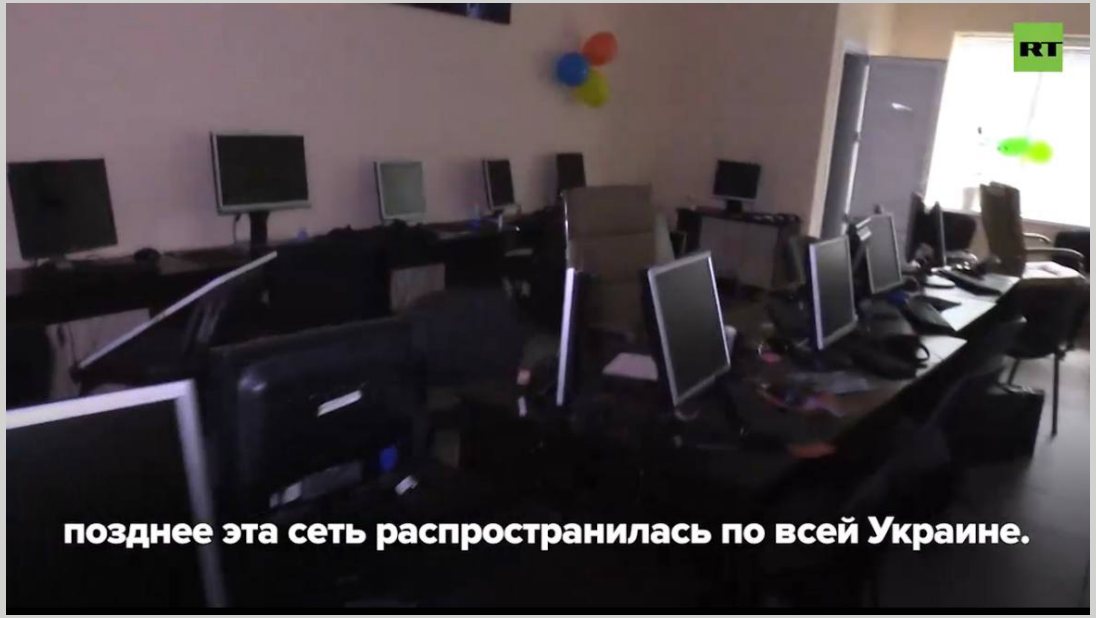
Тотальный прозвон всех имеющихся абонентов по нескольку раз звонками «службы безопасности банка» выработал привычное недоверие таким звонкам.

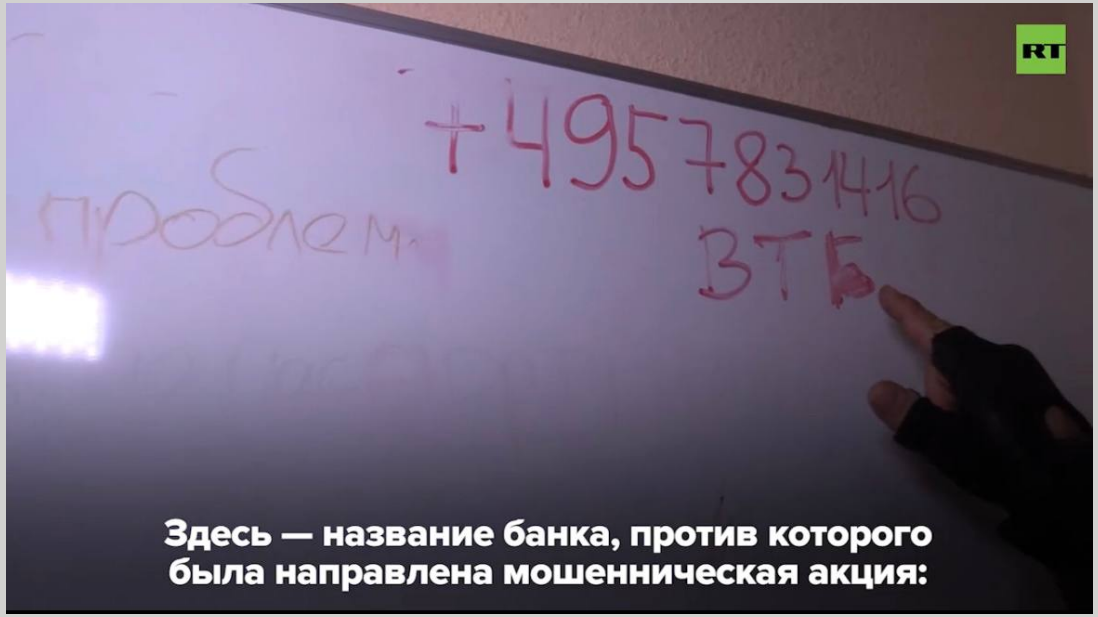
Приложения определения номера появились в массовых приложениях и социальных сетях.

Что случилось с 24 февраля?

«Служба безопасности» вышла из чата…

- Изменение целей колл-центров
- Отсутствие реакции жертв социалки
- Остался только целевой фишинг на торговых площадках





Тотальная автоматизация мошенничества

Роботизация звонков

- Повышение конверсии
- Мимикрия под сервисы банков
- Обмен базами
- Обход определителей номера

Автоматизация разворачивания

- Регистрация ресурсов
- Разворачивание сайтов
- Выкуп рекламы
- Защита от противодействия

Тотальная автоматизация мошенничества

Четкое разделение сервисов

- Получение данных
- Разворачивание сервисов
- Поддержка
- Социальные инженеры
- Технические средства хищения
- Обналичивание

Переиспользование инструментов

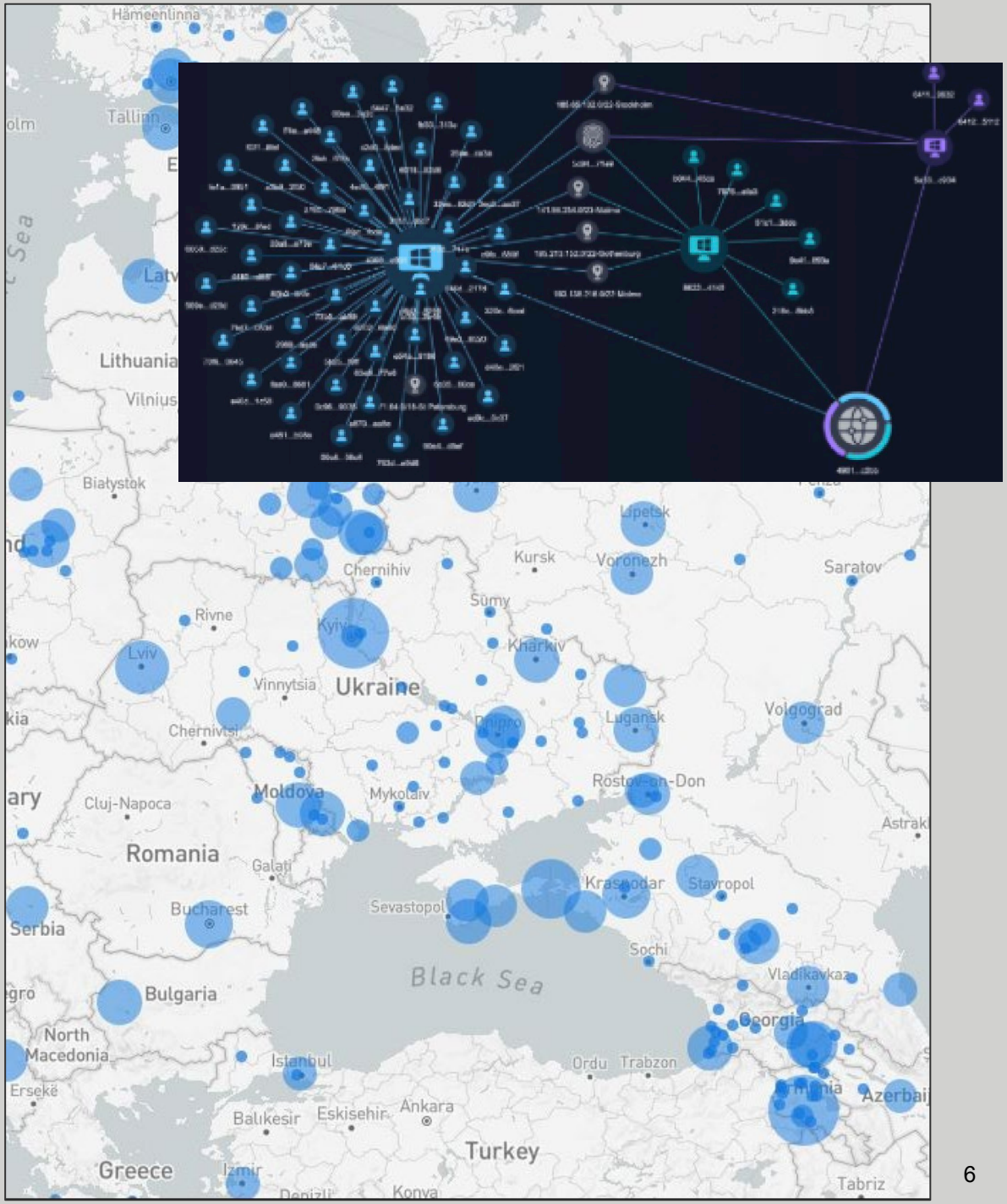
- Черный рынок решений
- Перепродажа успешно «отработавших» решений

Активное противодействие мошенников

- Уход от локальных провайдеров
  - Быть больше похожим на «клиента»
  - Использовать устройство клиента

- Защита своих сервисов
  - От противоатак и обхода модерации и поисковых систем (cloudflare,…)

- Подавление сервисов защиты
  - Пересобранные приложения
  - Блокировка сетевого трафика

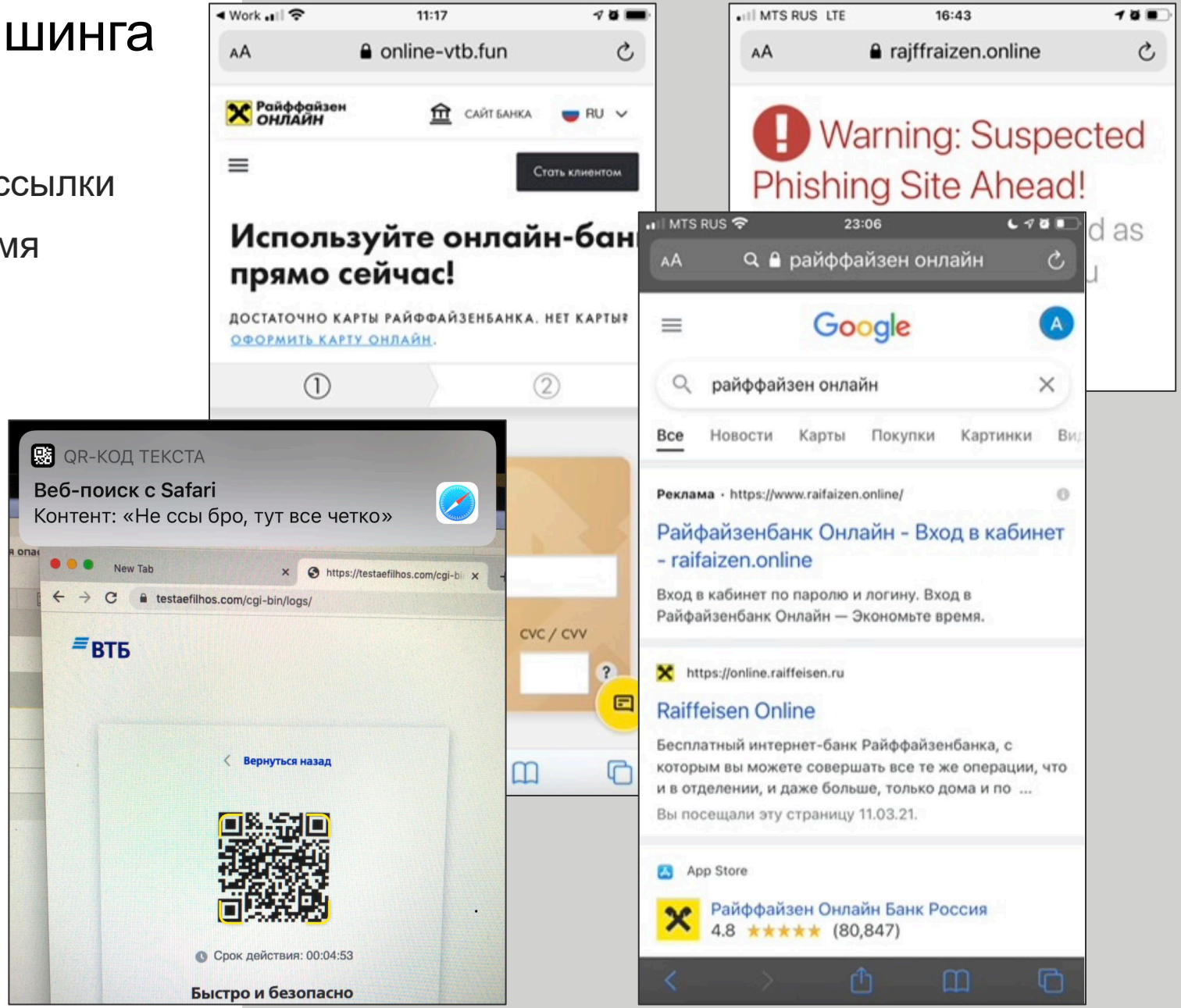


Реклама как двигатель фишинга

- Никто не использует сохраненные ссылки
- В браузере телефона разглядеть имя домена сложно
- Проверить сертификат – а что это?
- Все же выглядит очень похоже…

Проблема:

Время от запроса до блокировки ресурса составляет от 4 до 14 дней.



Что будет дальше?

- Фишинг
  - социальные сети
  - мессенджеры
- Атаки на API (СБПэй)
  - уязвимости / быстрое развитие

Новый день - новая угроза

- Возврат к веб-технологиям на мобильных устройствах
  - как защищать?
- Карты иностранных банков
  - выпуск карт / турпоездки
  - пополнение карт

Райффайзен БАНК

Спасибо!
Вопросы?

Александр Мотичев
Отдел противодействия кибермошенничеству

raif.ru

Просто. Четко.
Компетентно.