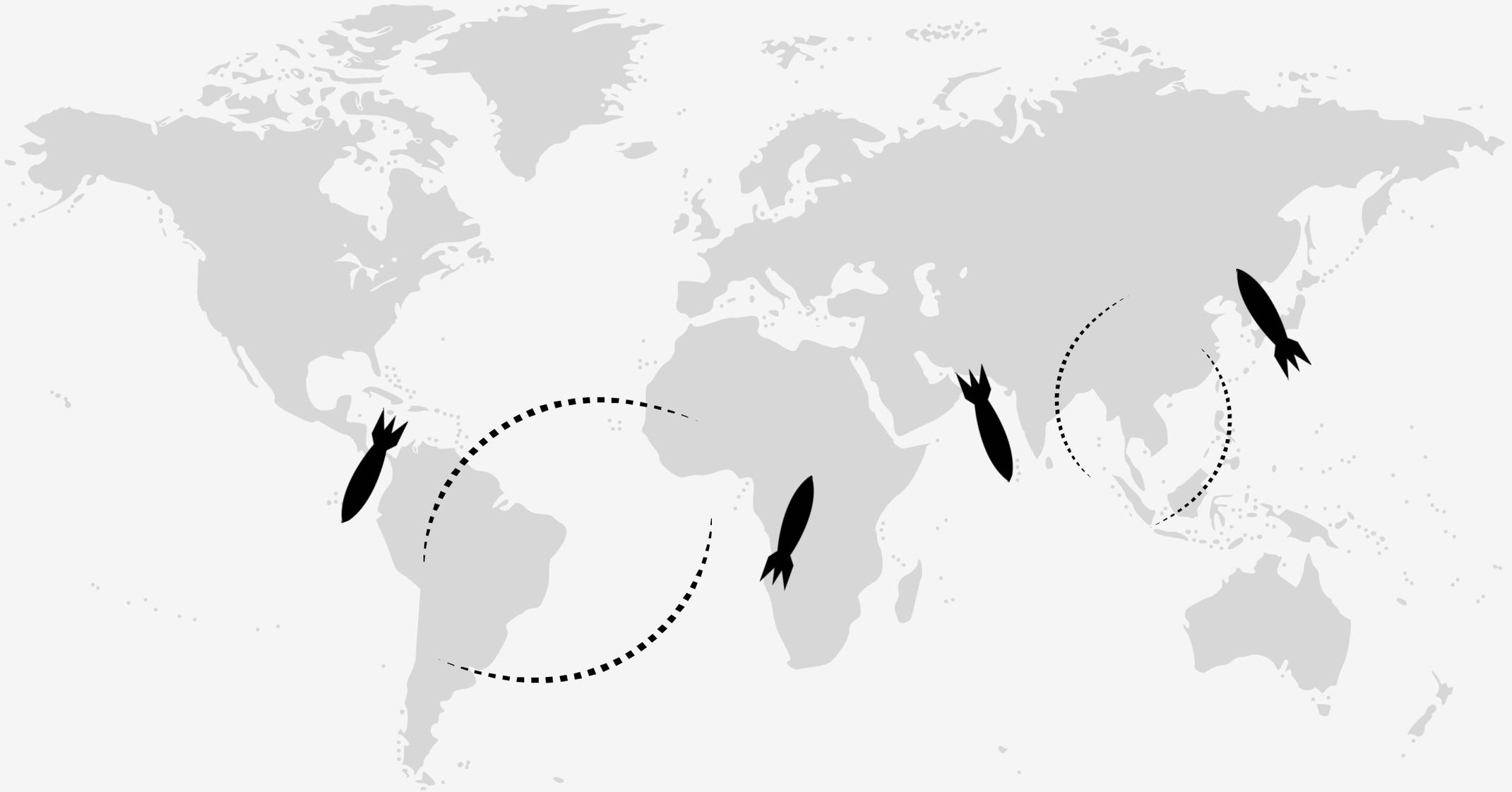
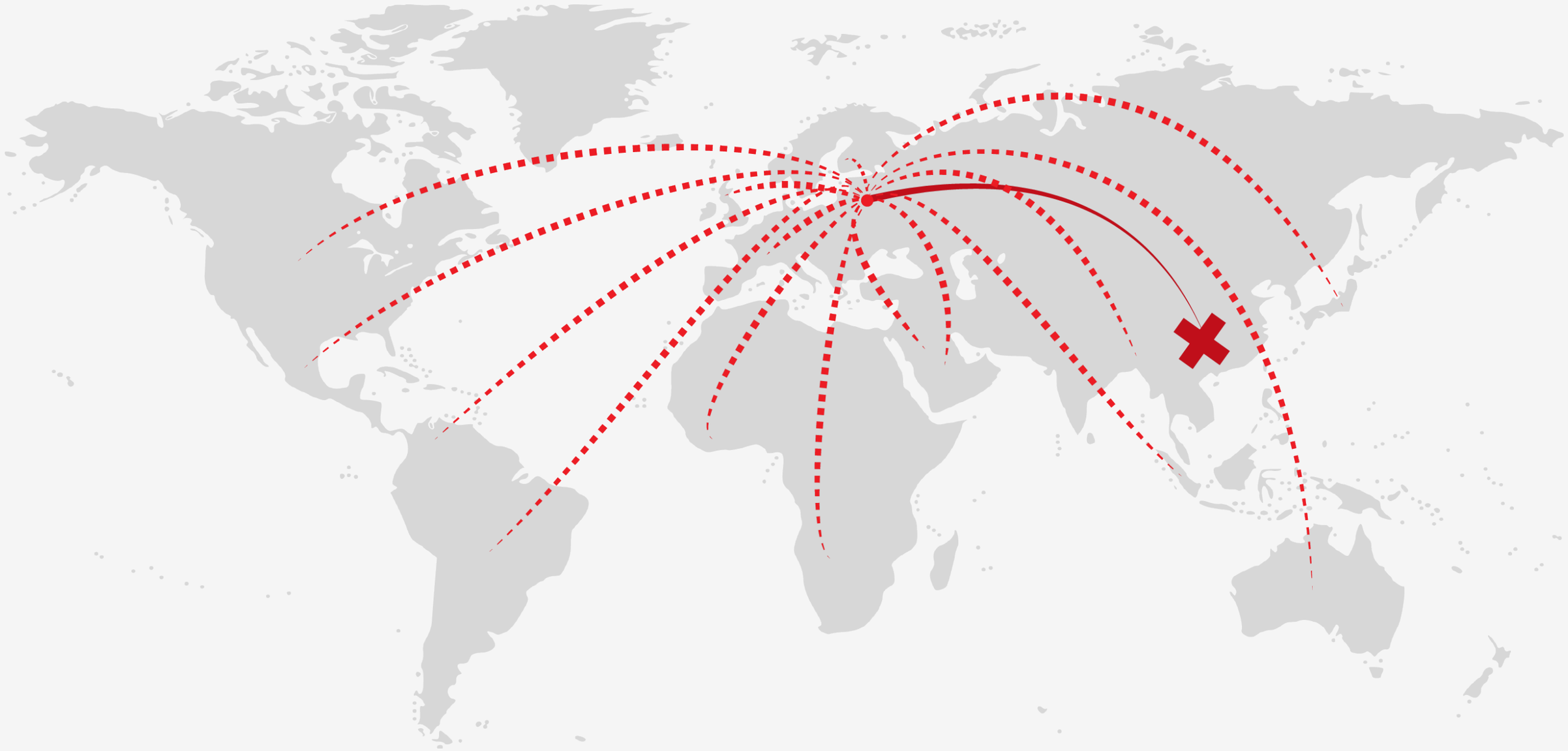
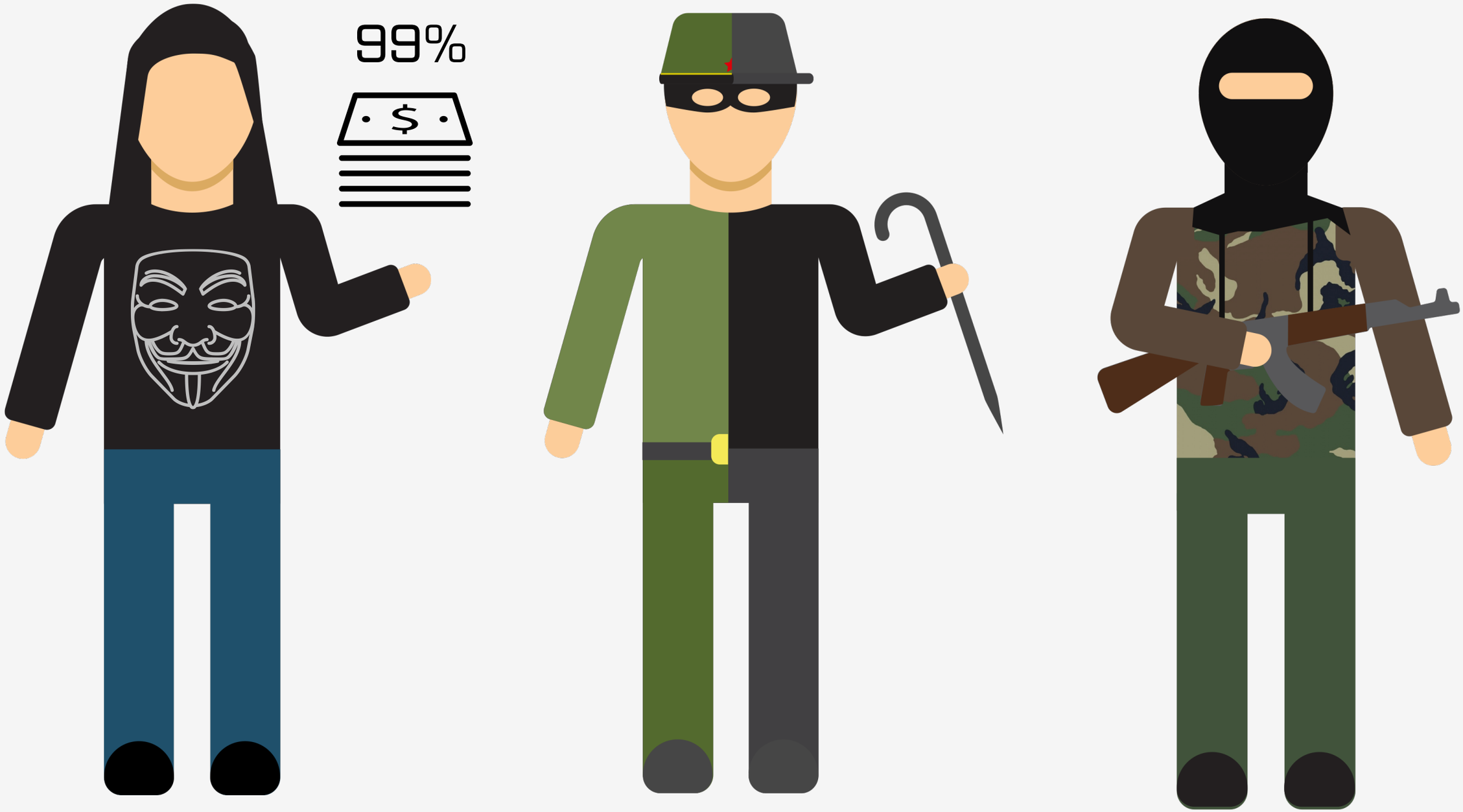
ТЕНДЕНЦИИ
РАЗВИТИЯ
ВЫСОКОТЕХНОЛОГИЧНЫХ
ПРЕСТУПЛЕНИЙ

HI-TECH CRIME TRENDS 2016

2015 Q2 — 2016 Q1






99%
$

АМПЛИФИКАЦИЯ

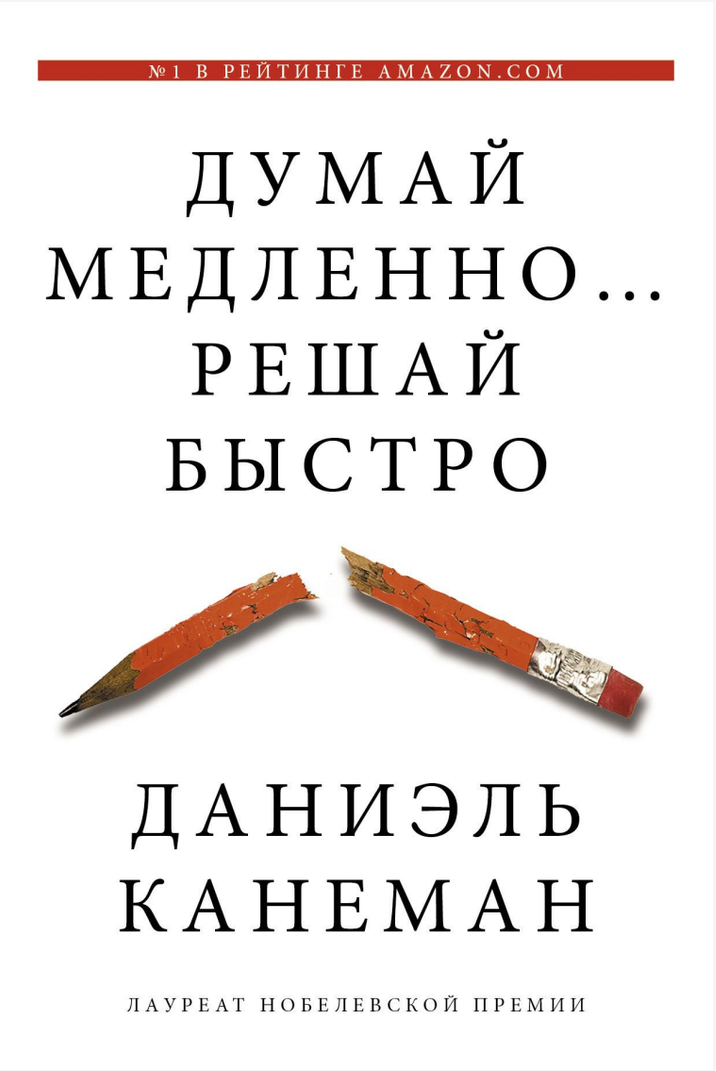
Чрезмерно детальное планирование
в условиях отсутствия в достаточном объёме
исходных данных и наличия сильно влияющих
на результат неопределенных или случайных
факторов

ПРЕДПОЧТЕНИЕ НУЛЕВОГО РИСКА

Предпочтение уменьшить какой-то один
маленький риск до нуля вместо того, чтобы
значительно уменьшить другой, больший риск

ЭВРИСТИКА ДОСТУПНОСТИ

Оценка как более вероятного того,
что более доступно в памяти



WW I

Лига наций

WW II

ООН

КАРИБСКИЙ КРИЗИС

Соглашения
о ядерном разоружении

?

Соглашения
о неиспользовании
кибервооружения

В феврале 2015 года группа Corkow получила контроль над брокерским терминалом одного из российских банков и выставила заявки на покупку и продажу валюты на сумму более $500 000 000.

В результате курс рубля на биржевых торгах снизился более чем на 15%.

АТАКА ДЛИЛАСЬ 14 МИНУТ, А ПОДГОТОВКА К НЕЙ – 6 МЕСЯЦЕВ.

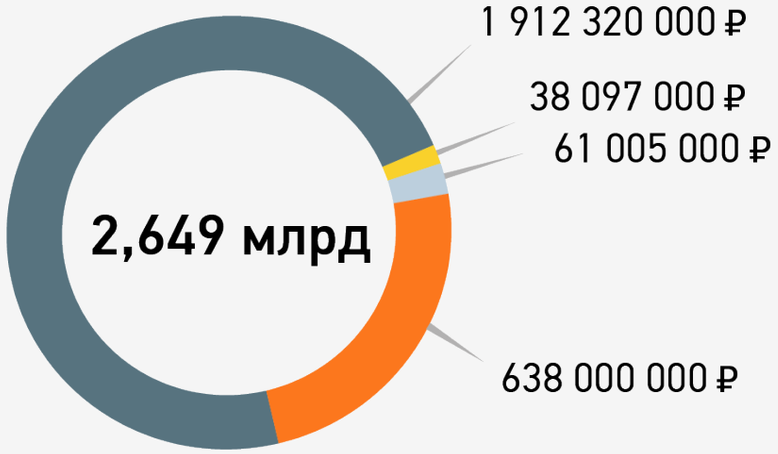
ТЕНДЕНЦИИ
РАЗВИТИЯ
ВЫСОКОТЕХНОЛОГИЧНЫХ
ПРЕСТУПЛЕНИЙ

HI-TECH CRIME TRENDS 2016

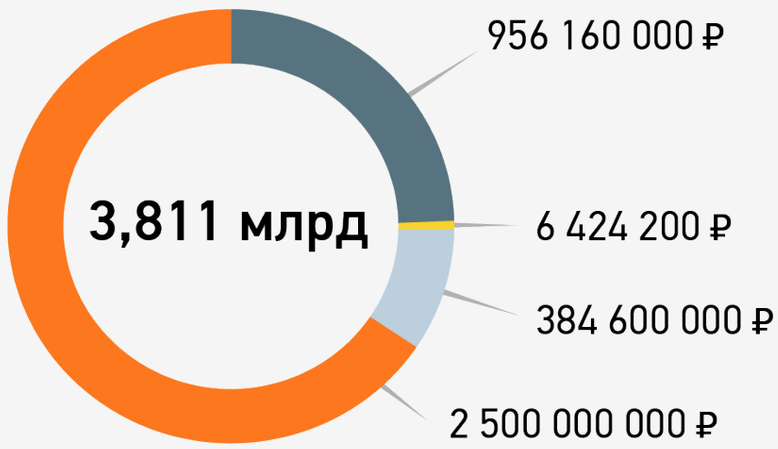
2015 Q2 — 2016 Q1

ОЦЕНКА РОССИЙСКОГО РЫНКА ХИЩЕНИЙ
ОСНОВНОЙ ДРАЙВЕР РОСТА – ЦЕЛЕВЫЕ АТАКИ

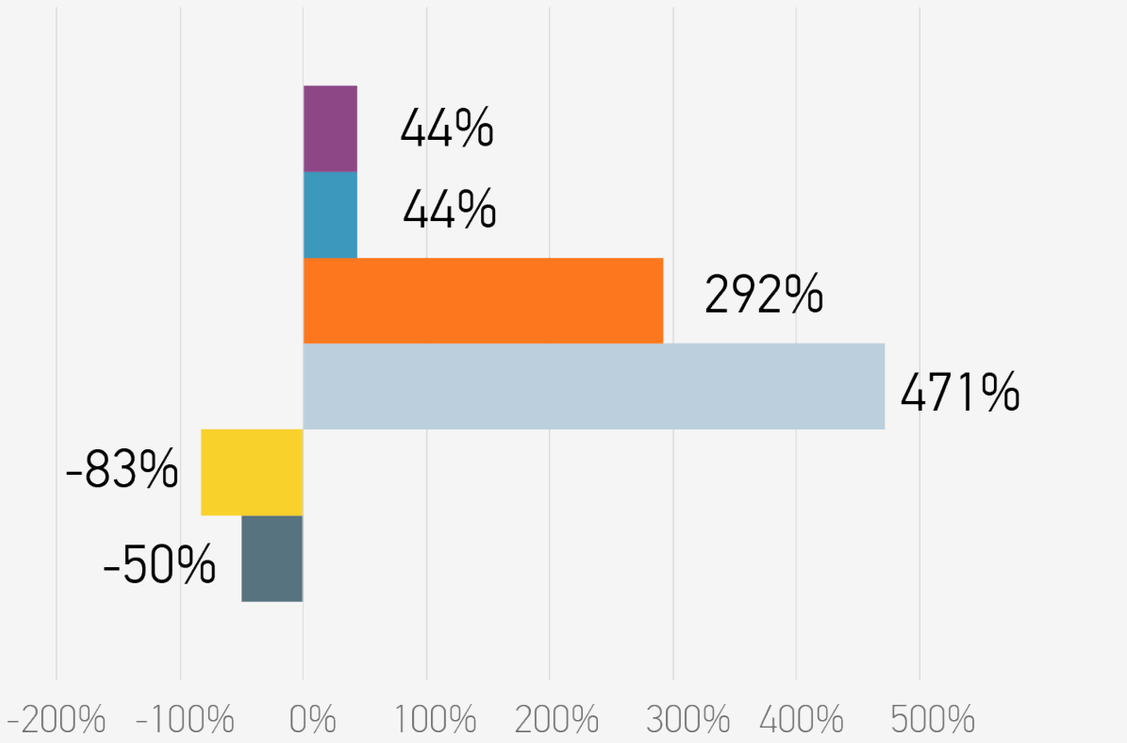
Q2 2014 - Q1 2015



Q2 2015 - Q1 2016



Изменение по отношению
к предыдущему периоду



- ХИЩЕНИЯ В ИНТЕРНЕТ-БАНКИНГЕ У ЮРИДИЧЕСКИХ ЛИЦ
- ХИЩЕНИЯ У ФИЗИЧЕСКИХ ЛИЦ С ТРОЯНАМИ ДЛЯ ПК
- ХИЩЕНИЯ У ФИЗИЧЕСКИХ ЛИЦ С ANDROID-ТРОЯНАМИ
- ЦЕЛЕВЫЕ АТАКИ НА БАНКИ
- ОБНАЛИЧИВАНИЕ ПОХИЩАЕМЫХ СРЕДСТВ
- ИТОГО

ТРЕНД №1
ГЛОБАЛЬНОСТЬ ЦЕЛЕВЫХ АТАК НА БАНКИ

2015-2016
ИЗВЕСТНЫЕ АТАКИ НА SWIFT:

Россия
Украина
Бангладеш
Эквадор
Филиппины
Вьетнам
Китай

2015-2016
ИЗВЕСТНЫЕ АТАКИ НА ПРОЦЕССИНГ:

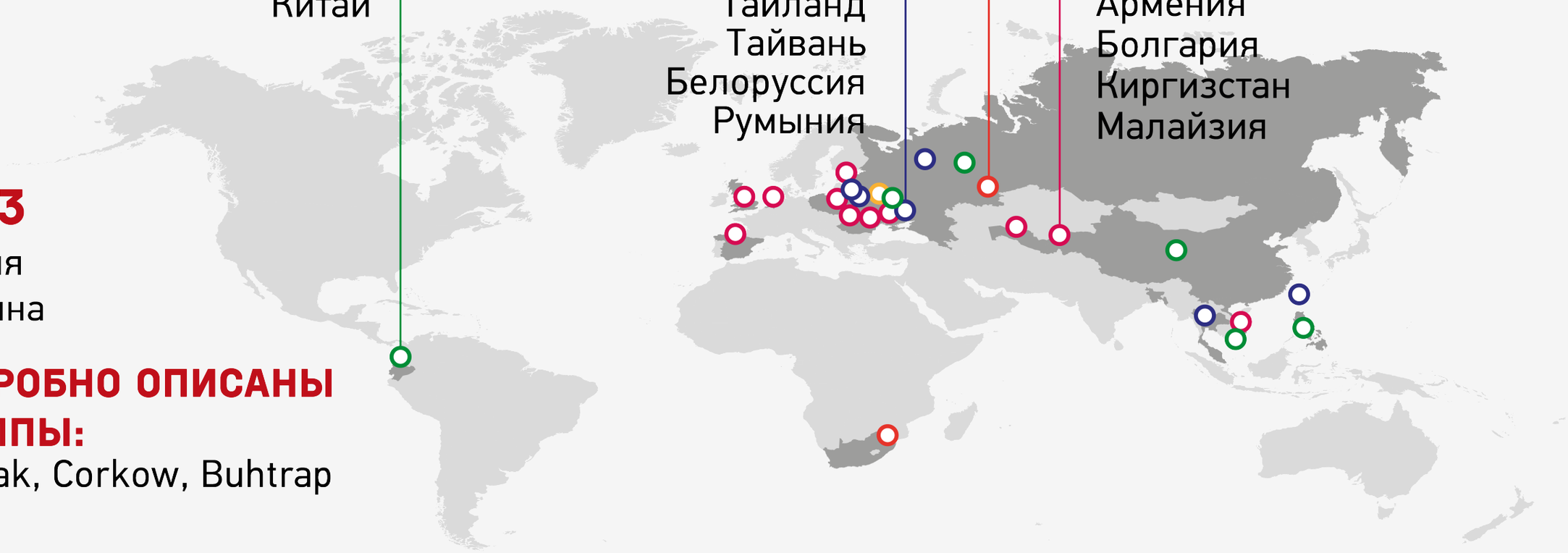
Россия
Южная Африка

2015-2016
ИЗВЕСТНЫЕ АТАКИ НА АТМ:

Россия
Украина
Таиланд
Тайвань
Белоруссия
Румыния

2015-2016
ИЗВЕСТНЫЕ ПОПЫТКИ АТАК:

Великобритания
Нидерланды
Испания
Польша
Эстонии
Молдавия
Грузия
Армения
Болгария
Киргизстан
Малайзия



2013

Россия
Украина

ПОДРОБНО ОПИСАНЫ ГРУППЫ:

Anunak, Corkow, Buhtrap

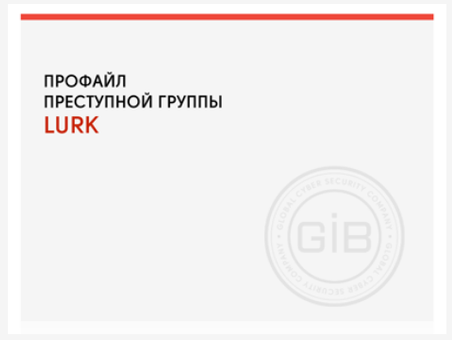
ТРЕНД №2
ТЕ, КТО АТАКОВАЛ КЛИЕНТОВ, ТЕПЕРЬ АТАКУЕТ БАНКИ

ТЕКУЩИЕ

скоро!

BUHTRAP

АРМ КБР

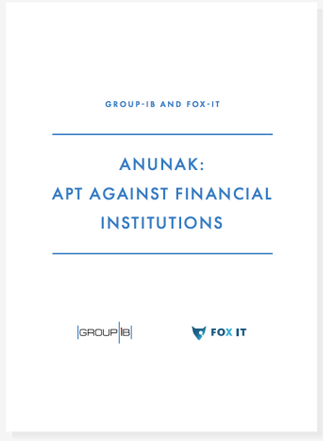


LURK

АРМ КБР

CORKOW

Карточный процессинг, банкоматы, биржевые терминалы



ANUNAK

АРМ КБР, SWIFT, банкоматы, платежные шлюзы, процессинг

GROUP-IB.RU/REPORTS

ПРОГНОЗ
ЦЕЛЕВЫЕ АТАКИ НА БАНКИ

СМЕНА ПРОФИЛЯ

Атакующие клиентов начнут атаковать банки

РАСШИРЕНИЕ ГЕОГРАФИИ

Атакующие российские банки продолжат экспансию на зарубежные рынки

РАСШИРЕНИЕ КОМПЕТЕНЦИЙ

Атакующие банкоматы начнут атаковать SWIFT

Аресты в России ускорят процесс

ФИШИНГОВЫЕ РАССЫЛКИ

Основной вектор первичного проникновения в сеть банка

ПРИВЛЕЧЕНИЕ ИНСАЙДЕРОВ

Активизируется поиск инсайдеров (контакты, запуск приложения, консультации по работе с системами)

ЛЕГАЛЬНЫЕ ИНСТРУМЕНТЫ

Для атак будут чаще использоваться легитимные или бесплатные программы

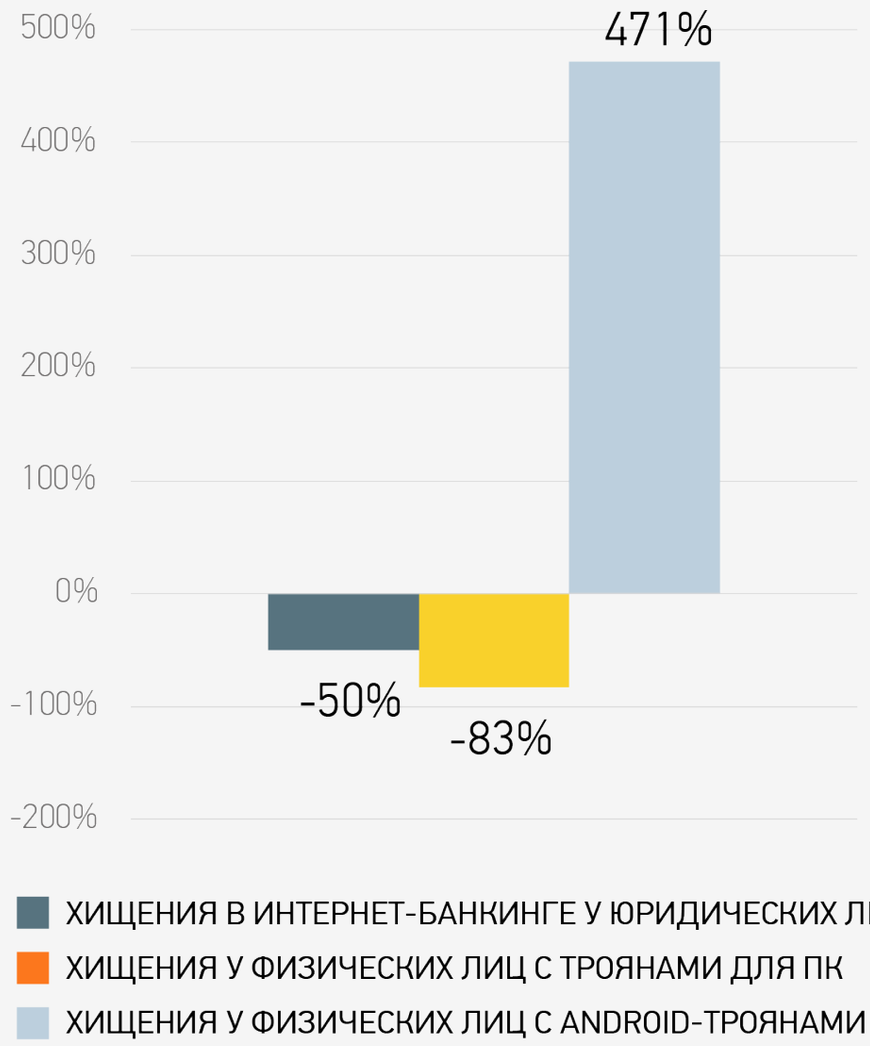
ТРЕНД №3

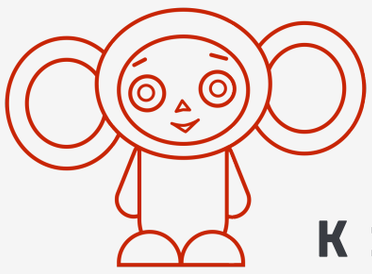
ЗАХВАТ РЫНКА ВИРУСОПИСАНИЯ ДЛЯ ПК РУССКОЯЗЫЧНЫМИ СПЕЦИАЛИСТАМИ

РОССИЯ

Buhtrap
Toplel
Ranbyus
RTM (new)
Jupiter (new)

Lurk
Corkow
Yebot
Kronos
Chtonic





К 16 ИЗ 19 ТРОЯНОВ ДЛЯ ПК, НАИБОЛЕЕ АКТИВНО ИСПОЛЬЗУЮЩИХСЯ ДЛЯ ХИЩЕНИЙ ПО ВСЕМУ МИРУ, ПРИЧАСТНЫ РУССКОЯЗЫЧНЫЕ ПРОГРАММИСТЫ

МИР

Panda Banker (new)
Shifu (new)
Midas bot (Jupiter) (new)
GozNym (new)
Sphinx (new)
Corebot (new)
Atmos (new)
Gozi (ISFB)
Dridex
Qadars
Gootkit
Vawtrak
Tinba
KINS (ZeusVM)
Citadel
Zeus
Quakbot (Qbot)
Retefe
Ramnit

ПРОГНОЗ
ЗАХВАТ РЫНКА ВИРУСОПИСАНИЯ ДЛЯ ПК РУССКОЯЗЫЧНЫМИ СПЕЦИАЛИСТАМИ

СОКРАЩЕНИЕ РОССИЙСКОГО РЫНКА

Количество групп, троянов и объем ущерба продолжат сокращаться

ОСВОЕНИЕ НОВЫХ РЫНКОВ

Трояны для иностранных банков будут появляться еще чаще

ПРОДАЖА ДЕЙСТВУЮЩИХ БОТ-СЕТЕЙ

Некоторые существующие бот-сети будут проданы менее опытным атакующим

ВЕБ-ИНЖЕКТЫ

Хищения продолжат автоматизироваться с помощью веб-инжектов

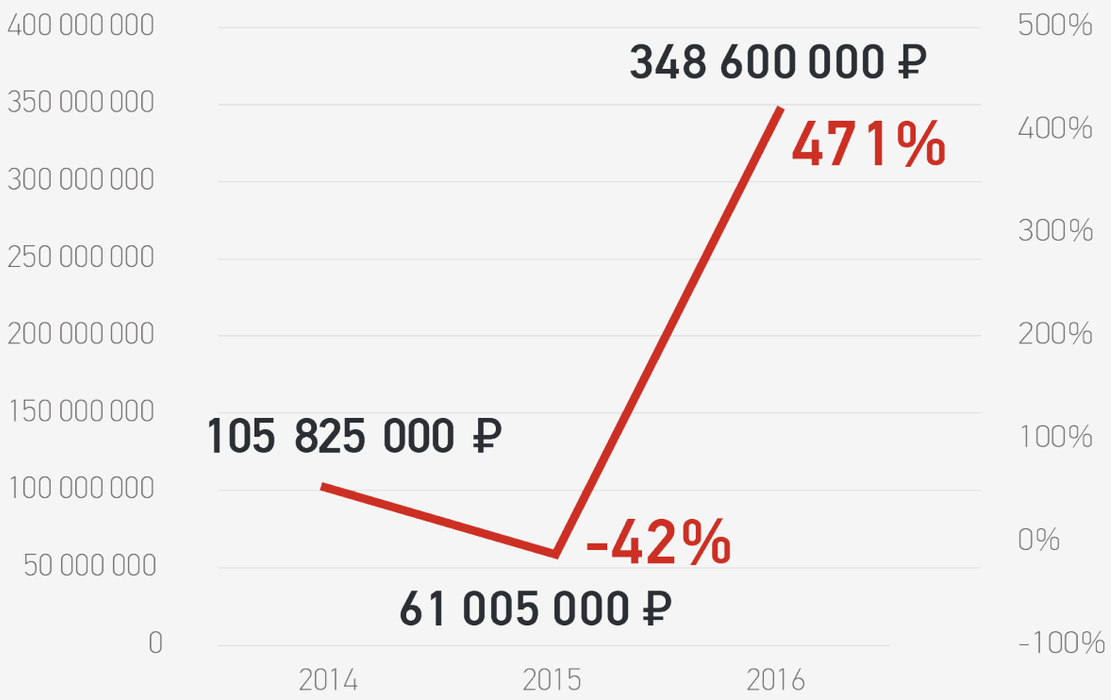
ВЕБ-ФЕЙКИ

Трояны расширят список атакуемых стран за счет простых веб-фейков

ПОЧТОВЫЙ СПАМ

Основной вектор распространения банковских троянов

ТРЕНД №4
ВСЕ УХОДЯТ НА ANDROID



РОССИЯ

Group 404
ApiMaps
Adabot
Cron1 (new)
FlexNet (new)
Agent.sx (new)
Agent.BID (new)
Honli (new)
Asucub (new)
FakeInst.ft (new)
GM bot (new)
Fake Marcher (new)
Cron2 (new)
Greff
March
Webmobil
Mikorta
MobiApps
Xruss
Tark
Sizeprofit

ЕВРОПА И США

Marcher 2.0 (new)
Xbot (new)
Abrvall (new)
Asacub (new)
Mbot 2.0 (new)
T00rb00r (new)
Marcher
GM-bot
Skunk
Bilal
Reich (Svpeng)

ТРЕНД №4
ВСЕ УХОДЯТ НА ANDROID

ЧТО ОБЕСПЕЧИЛО ВЗРЫВНОЙ РОСТ?

НОВЫЕ СХЕМЫ ХИЩЕНИЙ

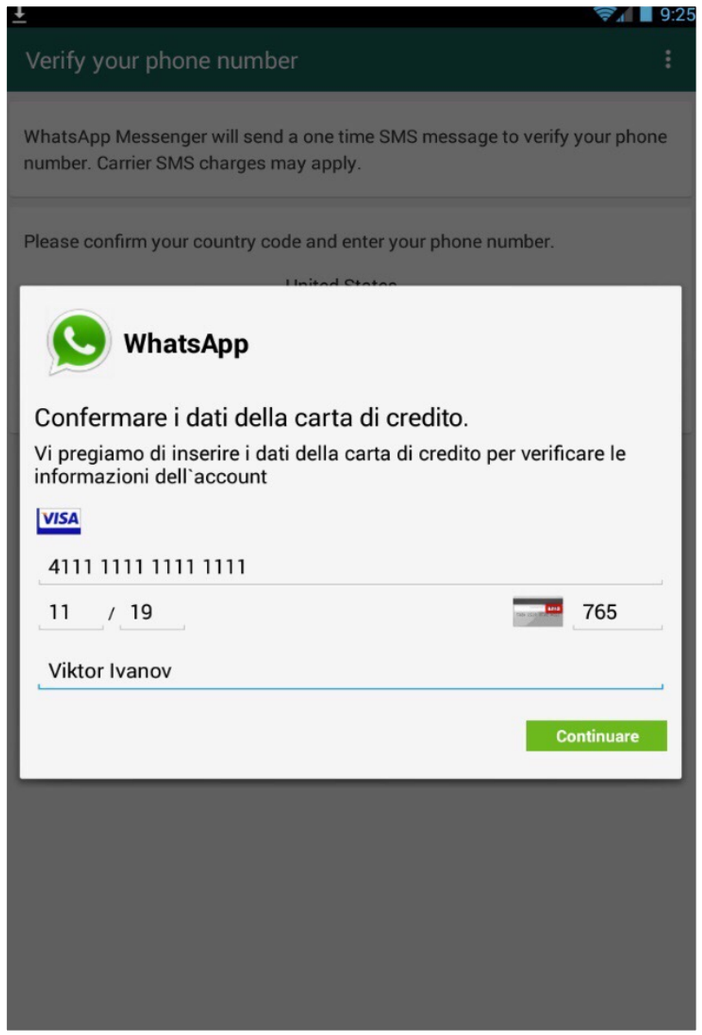
SMS-банкинг

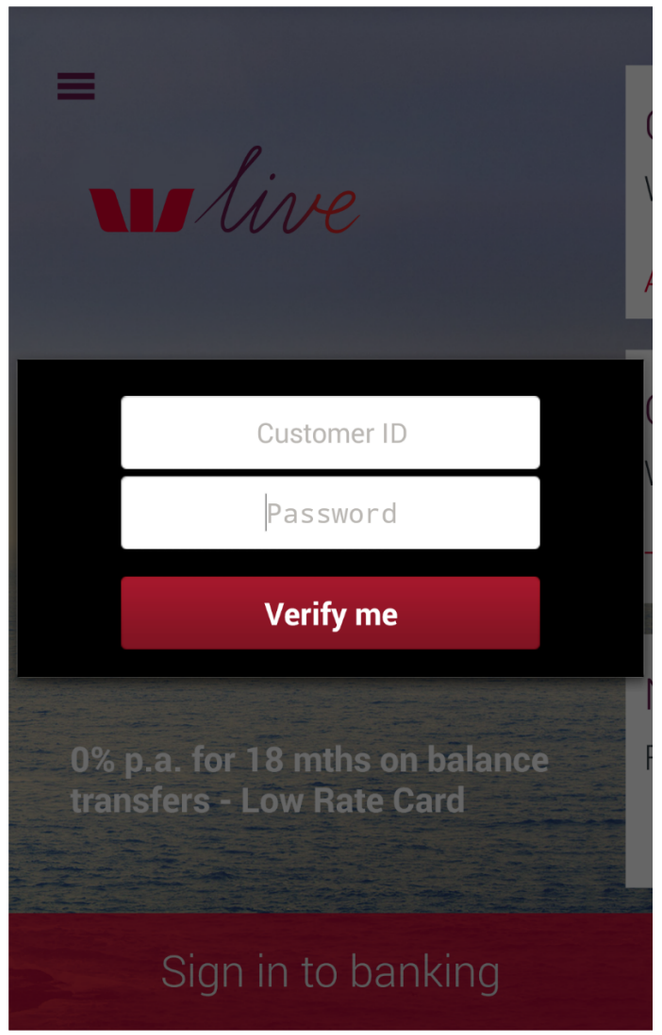
Переводы с карты на карту

Переводы через интернет банкинг

Поддельный мобильный банкинг

Активация мобильного приложения





ТРЕНД №4
ВСЕ УХОДЯТ НА ANDROID

ЧТО ОБЕСПЕЧИЛО ВЗРЫВНОЙ РОСТ?

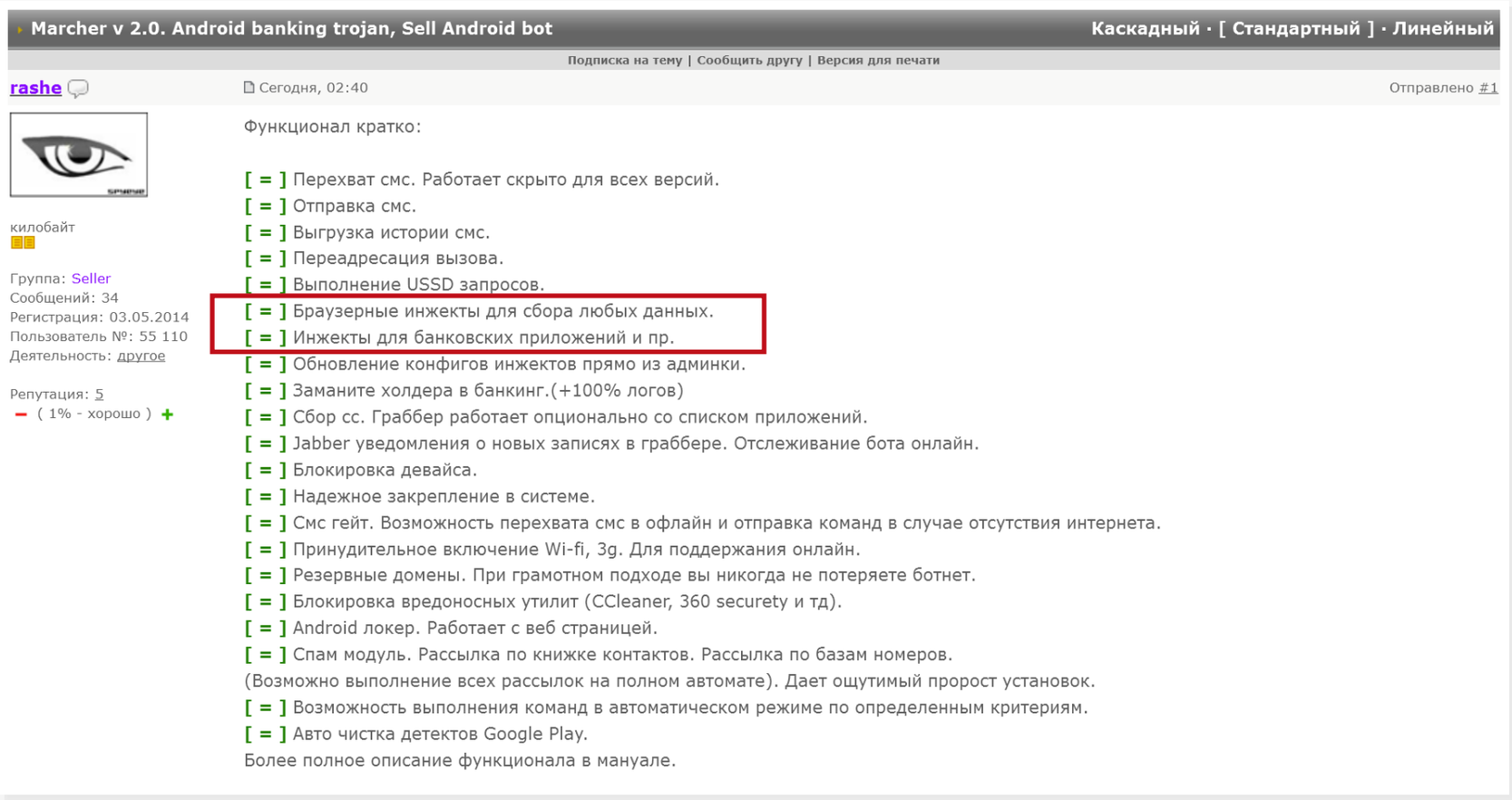
БОЛЕЕ СОВЕРШЕННЫЕ ТРОЯНЫ

Несколько стадий заражения

Защита кода и сетевых коммуникаций

Веб-фейки

Веб-инжекты



Marcher v 2.0. Android banking trojan, Sell Android bot

Каскадный · [Стандартный] · Линейный

Подписка на тему | Сообщить другу | Версия для печати

rashe

Сегодня, 02:40

Отправлено #1

килобайт

Группа: Seller
Сообщений: 34
Регистрация: 03.05.2014
Пользователь №: 55 110
Деятельность: другое

Репутация: 5
− (1% - хорошо) +

Функционал кратко:

[=] Перехват смс. Работает скрыто для всех версий.
[=] Отправка смс.
[=] Выгрузка истории смс.
[=] Переадресация вызова.
[=] Выполнение USSD запросов.
[=] Браузерные инжекты для сбора любых данных.
[=] Инжекты для банковских приложений и пр.
[=] Обновление конфигов инжектов прямо из админки.
[=] Заманите холдера в банкинг.(+100% логов)
[=] Сбор cc. Граббер работает опционально со списком приложений.
[=] Jabber уведомления о новых записях в граббере. Отслеживание бота онлайн.
[=] Блокировка девайса.
[=] Надежное закрепление в системе.
[=] Смс гейт. Возможность перехвата смс в офлайн и отправка команд в случае отсутствия интернета.
[=] Принудительное включение Wi-fi, 3g. Для поддержания онлайн.
[=] Резервные домены. При грамотном подходе вы никогда не потеряете ботнет.
[=] Блокировка вредоносных утилит (CCleaner, 360 securety и тд).
[=] Android локер. Работает с веб страницей.
[=] Спам модуль. Рассылка по книжке контактов. Рассылка по базам номеров.
(Возможно выполнение всех рассылок на полном автомате). Дает ощутимый пророст установок.
[=] Возможность выполнения команд в автоматическом режиме по определенным критериям.
[=] Авто чистка детектов Google Play.
Более полное описание функционала в мануале.

ТРЕНД №4
ВСЕ УХОДЯТ НА ANDROID

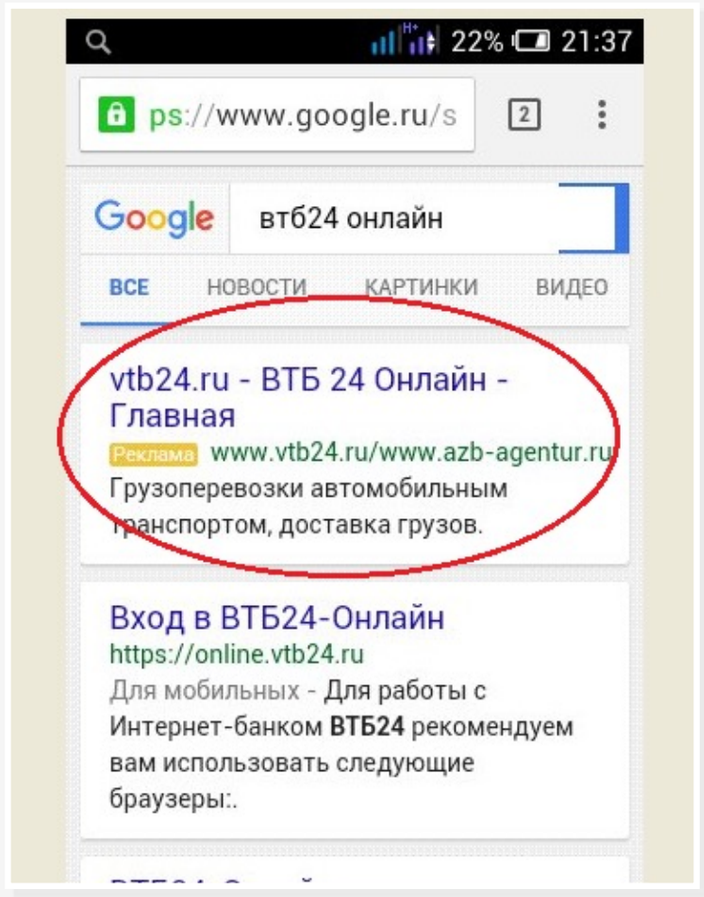
ЧТО ОБЕСПЕЧИЛО ВЗРЫВНОЙ РОСТ?

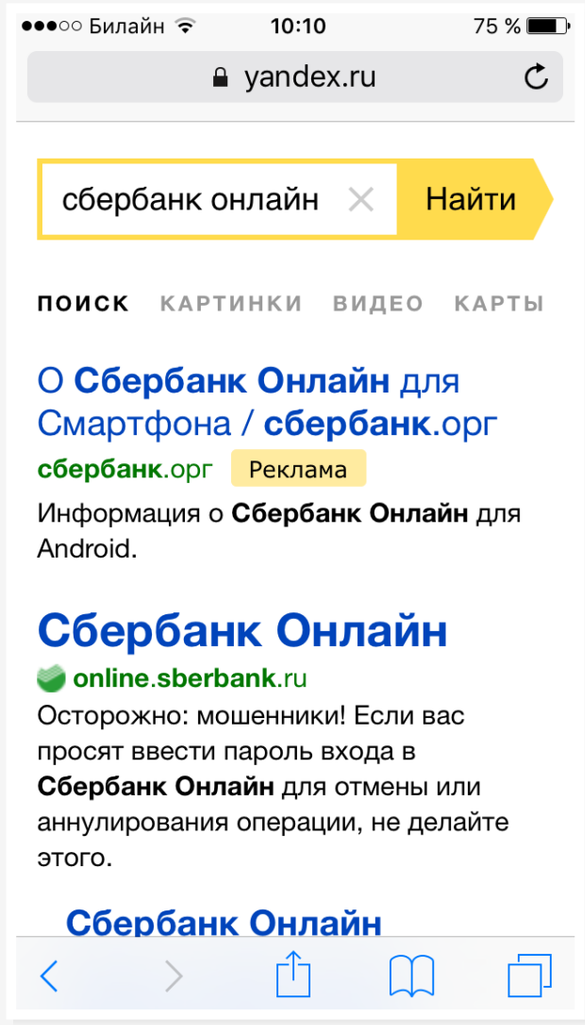
БОЛЕЕ ЭФФЕКТИВНОЕ РАСПРОСТРАНЕНИЕ

Контекстная реклама

Партнерские программы

Эксплойты





ПРОГНОЗ
РАСЦВЕТ БАНКОВСКИХ ТРОЯНОВ ДЛЯ ANDROID

ХИЩЕНИЯ У КОМПАНИЙ

Трояны адаптируются для хищений у юридических лиц

РОСТ УЩЕРБА

Средняя сумма ущерба вырастет за счет атак на компании

УСЛОЖНЕНИЕ ФУНКЦИОНАЛА

Трояны станут сложнее и будут еще больше похожи на трояны для ПК

НЕЗАМЕТНОЕ ЗАРАЖЕНИЕ

Появятся специальные наборы эксплойтов для Android

МОБИЛЬНЫЕ ВЕБ-ИНЖЕКТЫ

Появится аутсорсинг написания веб-инжектов под мобильные браузеры, больше троянов начнут поддерживать их

УЩЕРБ ОТ ANDROID-ТРОЯНОВ ПРЕВЫСИТ УЩЕРБ ОТ ТРОЯНОВ ДЛЯ ПК — ПРИОРИТЕТНАЯ УГРОЗА ДЛЯ БАНКОВ

ТРЕНД №5
ТОТАЛЬНАЯ АВТОМАТИЗАЦИЯ ХИЩЕНИЙ

✖ НА ПК

Активный автозалив

Пассивный автозалив

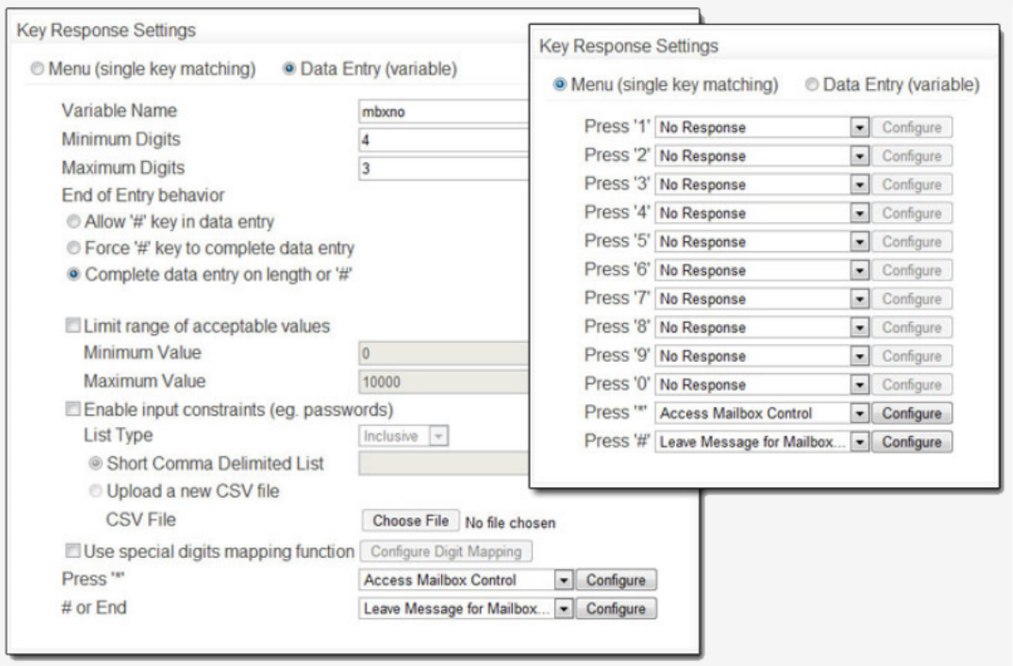
Все новые трояны поддерживают автозалив

Ranbyus внедрил автозалив через 1С

✖ НА ANDROID

Автоматический перевод через SMS-банкинг

Автоматический перевод с карты на карту



✖ ФИШИНГ

Обход SMS-подтверждений через диалоговые окна

✖ ВИШИНГ

Обход SMS-подтверждений через IVR

ПРОГНОЗ
АВТОМАТИЗАЦИЯ ХИЩЕНИЙ

АВТОЗАЛИВ НА ANDROID

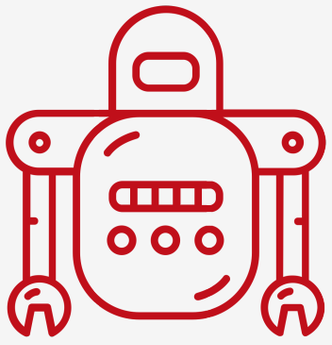
С помощью веб-инжектов можно будет подменять реквизиты платежа как у юридических, так и у физических лиц

АВТОМАТИЗАЦИЯ ФИШИНГА

Обход SMS-подтверждения сделает мобильные трояны угрозой №1 для большинства банков

РОБОТИЗАЦИЯ ВИШИНГА

Схема роботизированного вишинга адаптируется для обхода SMS-подтверждения и станет использоваться активнее



ПРИ РАСПРОСТРАНЕНИИ И АВТОМАТИЗАЦИИ ФИШИНГ И ANDROID-ТРОЯНЫ ОКОНЧАТЕЛЬНО ВЫТЕСНЯТ ТРОЯНЫ ДЛЯ ПК

ТРЕНД №6
IOT — ДРАЙВЕР РОСТА БОТ-СЕТЕЙ ДЛЯ DDOS-АТАК

2015
450 GBPS

ОТКАЗ ОТ УСИЛИТЕЛЕЙ

DNS, NTP, SSDP, CharGen и другие типы снижаются

2016
602 GBPS

ВОЗВРАТ К БОТ-СЕТЯМ

Бот-сети на Linux-серверах и IoT-устройствах популяризируются

09.2016
1 TBPS

ПУБЛИКАЦИЯ ИСХОДНЫХ КОДОВ

Lizard Stresser и Mirai опубликованы в открытом доступе

IOT-УСТРОЙСТВА — ИДЕАЛЬНЫЕ БОТЫ

Динамические IP-адреса

Не имеют антивирусов

Круглосуточный доступ в сеть

Сложно обновлять и устранять известные уязвимости

Пароли по умолчанию

ТРЕНД №7
ШИФРОВАЛЬЩИКИ — ЛАВИНООБРАЗНАЯ УГРОЗА

ОСНОВНАЯ ЦЕЛЬ — КОРПОРАТИВНЫЙ СЕКТОР

Покупают доступ к важным данным

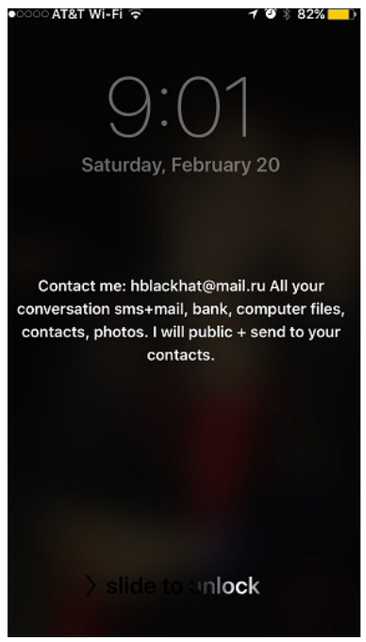
Сканируют и подбирают пароли от серверов

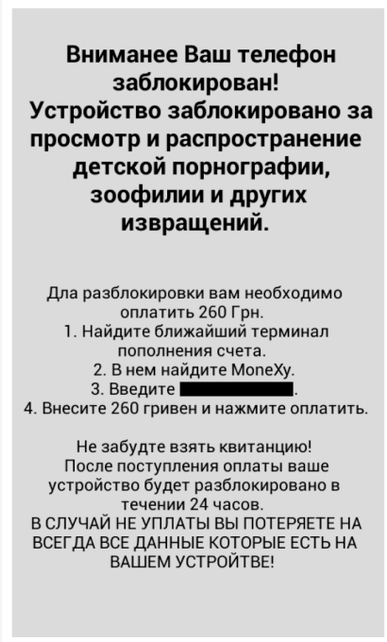
Шифруют Windows и Linux-серверы

README_FOR_DECRYPT-2.txt

```
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
generated for this computer.

To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow to decrypt the files, located on a secret
server at the Internet. After that, nobody and never will be able to restore files...

To obtain the private key and php script for this computer, which will automatically decrypt
files, you need to pay 1 bitcoin(s) (~420 USD).
Without this key, you will never be able to get your original files back.



_____

!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
WEBSITE: https://z54n57pg2el6uze2.onion.to

INSTRUCTION FOR DECRYPT:
```

АКТИВНЫЕ ЭКСПЕРИМЕНТЫ С МОБИЛЬНЫМИ И IOT-УСТРОЙСТВАМИ





ПРОГНОЗ
РОСТ ИНЦИДЕНТОВ С ШИФРОВАЛЬЩИКАМИ

РАСШИРЕНИЕ СПЕКТРА ЦЕЛЕЙ

Мобильные, IoT-устройства, облачные хранилища

ТОЧЕЧНАЯ НАПРАВЛЕННОСТЬ

Цели – компании с критичными бизнес-процессами, которые не могут позволить себе тратить время их на восстановление

УВЕЛИЧЕНИЕ СРЕДНЕГО ЧЕКА

Благодаря болеет целенаправленному распространению вымогателей по корпоративному сектору, размер требуемого выкупа увеличится

ЧЕРВИ

Распространение по сети с помощью червя для большего покрытия и ущерба

ОТВЛЕЧЕНИЕ ВНИМАНИЯ

Будут использоваться при целевых атаках для отвлечения внимания, как раньше было с DDoS

УВЕЛИЧЕНИЕ ЧИСЛА ИНЦИДЕНТОВ СТИМУЛИРУЕТ РАЗВИТИЕ СТРАХОВАНИЯ, ЧТО ЕЩЕ БОЛЬШЕ ПОДСТЕГНЕТ АТАКУЮЩИХ

ТРЕНД №8

УВЕЛИЧЕНИЕ ЧАСТОТЫ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

19 декабря 2014, 12:36 Виктор Степанов 4 732 35

Хакеры вывели из строя печи на металлургическом заводе в Германии

Группе неизвестных хакеров удалось взломать систему управления печами на металлургическом заводе в Германии и вывести из строя механизм их выключения. Об этом сообщает The Wall Street Journal.

Твитнуть | Поделиться | Поделиться

ВЕСТИ.RU Новости Видео Фотолента Трансляции

Новости | В мире Все видео этой рубрики

5 марта 2016 19:21

К взлому украинской энергосети хакеры готовились полгода

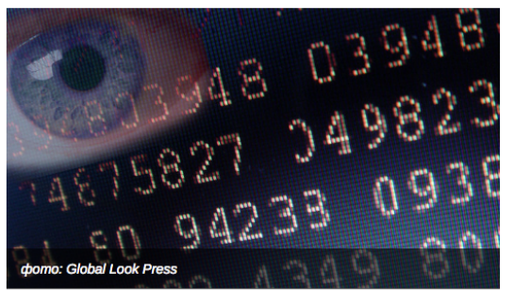


фото: Global Look Press

INDEPENDENT News Voices Culture Lifestyle Tech Sport Daily Edition

News › World › Americas

Bowman Avenue Dam: US in fear of new cyber attack as dam breach by Iranian hackers is revealed

It is reported that on 12 occasions in the last decade hackers gained top-level access to key pow networks

David Usborne US Editor | @dusborne | Monday 21 December 2015 | 6 comments

Ad

241 shares

Хакеры атаковали аэропорт «Борисполь»

Алексей Бондаренко 18 Января 2016 4694

Согласно информации Reuters, на прошлой неделе хакеры атаковали информационную систему главного украинского аэропорта — «Борисполь». Об этом информагентству сообщили украинские чиновники. По их словам, атака была запущена с серверов, расположенных на территории России.

Указ Президента України № 15/2015 "Про часткову мобілізацію" від 14.01.15 р. - Mozilla Thunderbird

Get Messages | Write | Chat | Address Book | Tag

From info@rada.gov.ua

Subject Указ Президента України № 15/2015 "Про часткову мобілізацію" від 14.01.15 р. 24.03.15 11:44

To [redacted]

Reply | Reply All | Forward | Other Actions

Відповідно до Указу Президента України № 15/2015 "Про часткову мобілізацію" від 14.01.15 р. з метою підтримання бойової і мобілізаційної готовності Збройних Сил України та інших військових формувань проводиться мобілізація громадян України.
Керівникам організацій необхідно надати списки співробітників організацій за зразком (Додаток 1) до органів місцевого управління. Списки категорій громадян, які не підлягають мобілізації представлені у додатку 2. Указ Президента України та порядок надання інформації представлені у додатку 3.

1 attachment: Додаток1.xls 718 KB Save

Додаток1.xls 718 KB

Вт 19.01.2016 17:51

Ukrenergo <info@ukrenergo.energy.gov.ua>

УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025

Кому [redacted]

Сообщение | Ocenka.xls (816 Кбайт)

Відповідно до положень Закону України «Про засади функціонування ринку електричної енергії України» та «Порядку підготовки Системним оператором плану розвитку Об'єднаної енергетичної системи України на наступні десять років», затвердженого наказом Міністерства енергетики та вугільної промисловості України від 29.09.2014 № 680, системним оператором було розроблено та розміщено на офіційному сайті компанії проект «Плану розвитку ОЕС України на 2016 – 2025 роки».
Проект Плану розвитку знаходиться в додатку до листа.
На виконання пункту 5 положення Порядку підготовки 20 січня 2016 року о 14-00 в адміністративному приміщенні ПС 750 кВ «Київська» (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б) будуть проводитись громадські обговорення та консультації щодо проекту Плану розвитку.

Державне підприємство Національна енергетична компанія УКРЕНЕРГО

ТРЕНД №9
БОЛЬШЕ ИНСТРУМЕНТОВ ДЛЯ ЦЕЛЕВЫХ АТАК И ШПИОНАЖА

НА УРОВНЕ ПРОВАЙДЕРА

Что нужно:
Доступ к маршрутизатору или своя ASN

Что дает:
Доступ ко всему трафику
Возможность расшифровывать SSL
Получение доступа к логинам и паролям внешних систем

С ПОМОЩЬЮ ANDROID-ТРОЯНОВ

Что дает:
Доступ к геопозиции
Перехват голоса
Перехват SMS
Доступ к мессенджерам, фотографиям, файлам
Отправка USSD-команд
Восстановление паролей
Доступ к облачному хранилищу

НА УРОВНЕ МОБИЛЬНОГО ОПЕРАТОРА

Что нужно:
Доступ к SS7 Hub или лицензия на платный сервис (Defentek, Verint, CleverSig, Circles, Cobham)

Что дает:
Доступ к геопозиции
Перехват голоса
Перехват SMS
Отправка USSD-команд

ПРОГНОЗ
АТАКИ НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

ОТКРЫТОСТЬ ИНФОРМАЦИИ

Сведения об успешных атаках начнут чаще просачиваться в СМИ из-за политического подтекста

ПОПУЛЯРИЗАЦИЯ

Резонанс от успешных атак будет привлекать к ним большее внимание киберармий и террористов

КИБЕРАРМИИ

Одной из целей киберармий будут объекты критической инфраструктуры

Цель: шпионаж и возможность контроля

ТЕРРОРИСТЫ

Киберячейки террористов начнут атаки на критические объекты

Цель: общественный резонанс, человеческие жертвы

АРЕСТЫ И ВЕРБОВКА

Аресты людей, причастных к целевым атакам на коммерческие организации, будут заканчиваться их вербовкой

ОНЛАЙН-РЕКРУТИНГ

Террористы будут вести онлайн-пропаганду и рекрутинг специалистов, способных проводить целевые атаки

СТРУКТУРА GROUP-IB

ПРЕДОТВРАЩЕНИЕ

Аудит информационной безопасности

AntiPiracy

Brand Protection

РЕАГИРОВАНИЕ

Центр круглосуточного реагирования на инциденты ИБ CERT-GIB

РАССЛЕДОВАНИЕ

Компьютерная криминалистика и исследование вредоносного кода

Расследование инцидентов ИБ

Независимые финансовые и корпоративные расследования

СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

Киберразведка
Threat Intelligence

Обнаружение целевых атак
TDS
TDS Polygon

Выявление хищений и мошенничеств на этапе подготовки
Secure Bank
Secure Portal

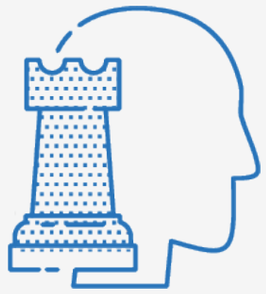
УНИКАЛЬНАЯ РЕСУРСНАЯ БАЗА, НАКОПЛЕННАЯ ЗА 13 ЛЕТ РАБОТЫ

Сбор данных об угрозах в ключевых регионах происхождения

Россия и Восточная Европа, Юго-Восточная Азия, Ближний Восток

ИНФРАСТРУКТУРА

- Распределенная сеть мониторинга и HoneyNet-ловушек
- Аналитика бот-сетей
- Трекеры сетевых атак
- Мониторинг хакерских форумов и закрытых сетевых сообществ
- Данные сенсоров TDS
- Система поведенческого анализа



HUMAN INTELLIGENCE

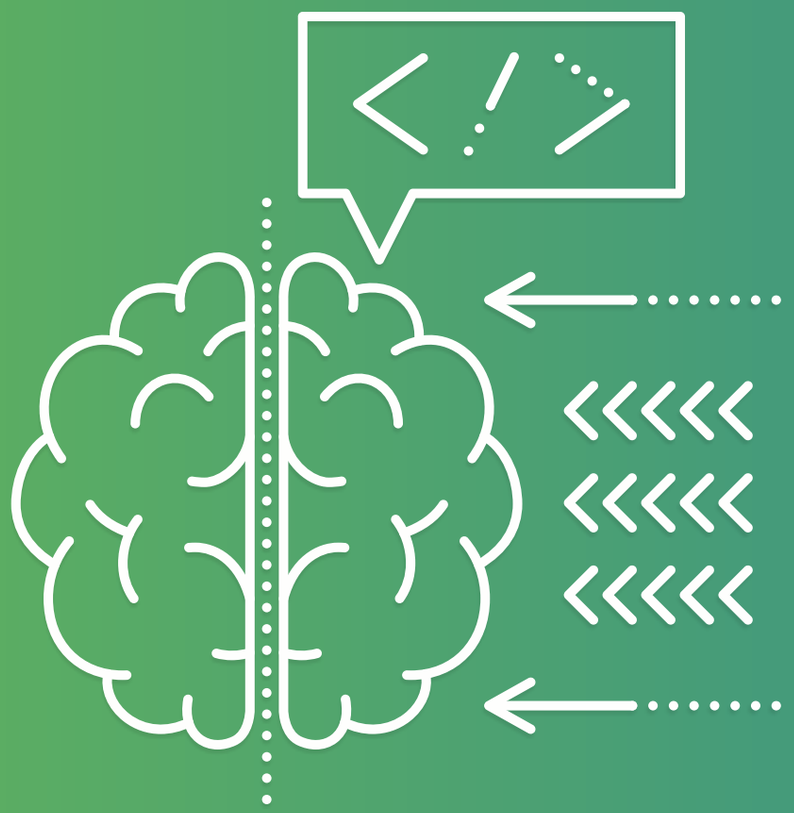
- Результаты экспертиз Лаборатории Group-IB
- Материалы расследований
- Мониторинг и анализ вредоносных программ
- База обращений и практика реагирования на инциденты CERT-GIB
- Результаты аудита
- Целевая аналитика Group-IB

ОБМЕН ДАННЫМИ

- Команды реагирования CERT
- Регистраторы и хостинг-провайдеры
- Производители средств защиты
- Организации и объединения по противодействию киберугрозам
- Europol, Interpol и правоохранительные органы

TDS Polygon

Выявление ранее неизвестного
вредоносного кода с использованием
передовых алгоритмов машинного обучения



МАШИННЫЙ ИНТЕЛЛЕКТ ПОМОГАЕТ ВЫЯВИТЬ

- фишинговые рассылки
- атаки на браузер
- атаки с использованием ранее неизвестных вредоносных программ и инструментов