«Цифровые» нарушения, направленные на устранение/ограничение конкуренции, способы выявления и сбора доказательств

Александр Сушко
Руководитель офиса, Group-IB
sushko@group-ib.by

Развитие информационно-коммуникационных технологий

Масштаб и количество киберпреступлений, устройств, пользователей и потерпевших

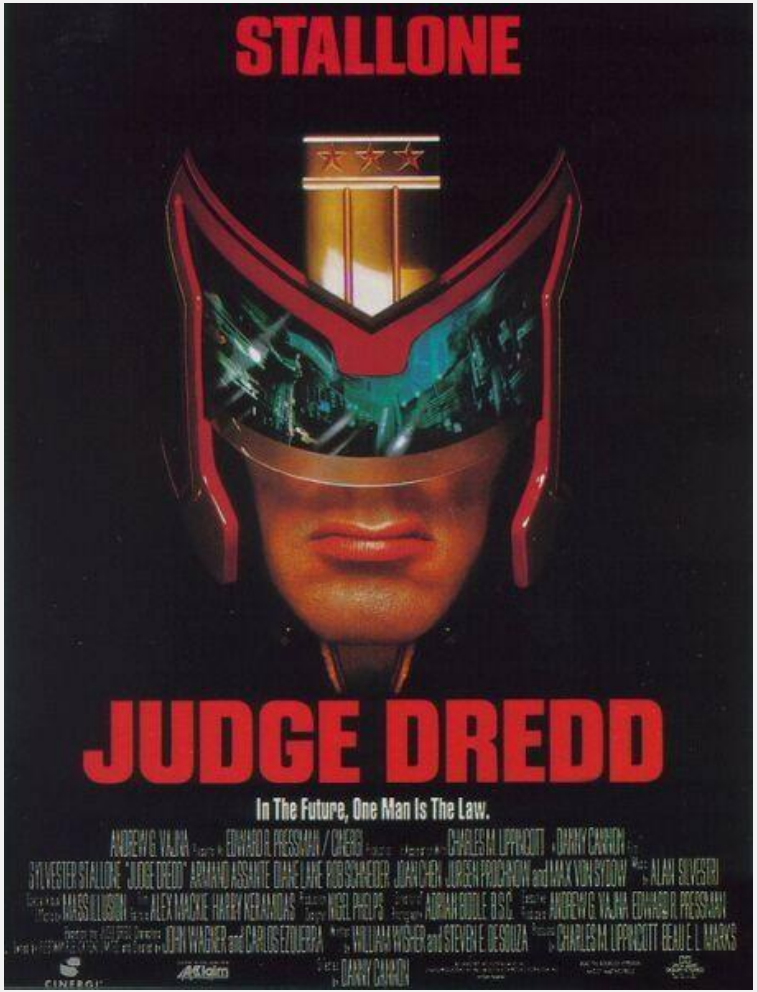
Транснациональность и экстерриториальность, юрисдикция

Big data

Cloud

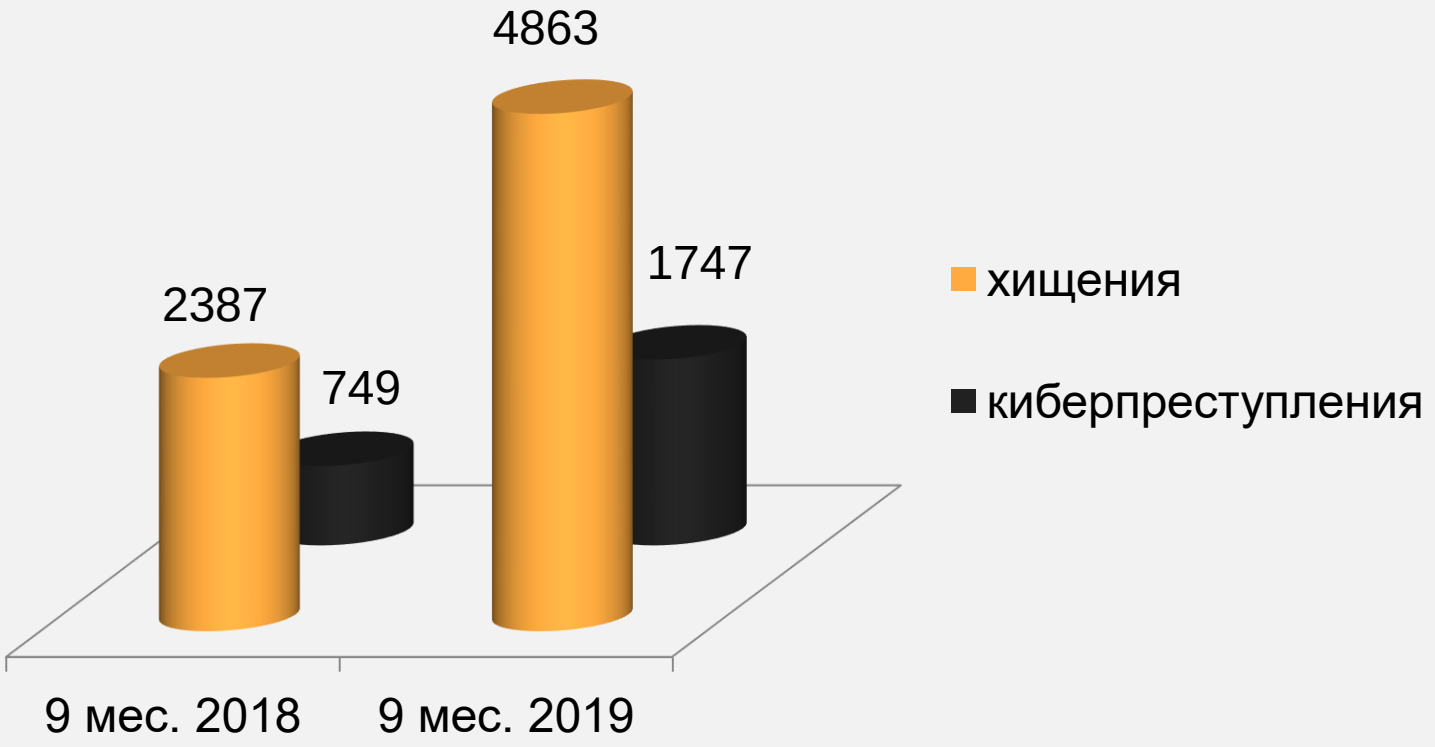
Интернет вещей

Цифровизация


STALLONE
JUDGE DREDD
In The Future, One Man Is The Law.


WORLD OF TANKS

Республика Беларусь



О компании

Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий

1000+

успешных расследований по всему миру, 150 особо сложных уголовных дел

$300 млн

возвращено клиентам Group-IB благодаря нашей работе

EUROPOL INTERPOL

Официальный партнер EUROPOL и INTERPOL

OSCE

Рекомендована Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

BUSINESS INSIDER

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider

Forrester Gartner

Threat Intelligence от Group-IB – в числе лучших мировых систем по оценке Forrester и Gartner

WORLD ECONOMIC FORUM

Постоянный член Всемирного экономического форума

IDC

Лидер российского рынка по исследованию киберугроз

Наши продукты и услуги

Система раннего предупреждения

- Threat Detection System
- Threat Intelligence
- Secure Bank
- Secure Portal

Расследование инцидентов

- Компьютерная криминалистика и исследование вредоносного кода
- Расследование инцидентов ИБ
- Независимые финансовые и корпоративные расследования

Предотвращение угроз

- Аудит безопасности
- Compromise Assessment
- Red Teaming
- Brand Protection
- Anti-Piracy

Реагирование 24/7/365

- Центр реагирования на инциденты информационной безопасности CERT-GIB

Отчеты и публикации

2014

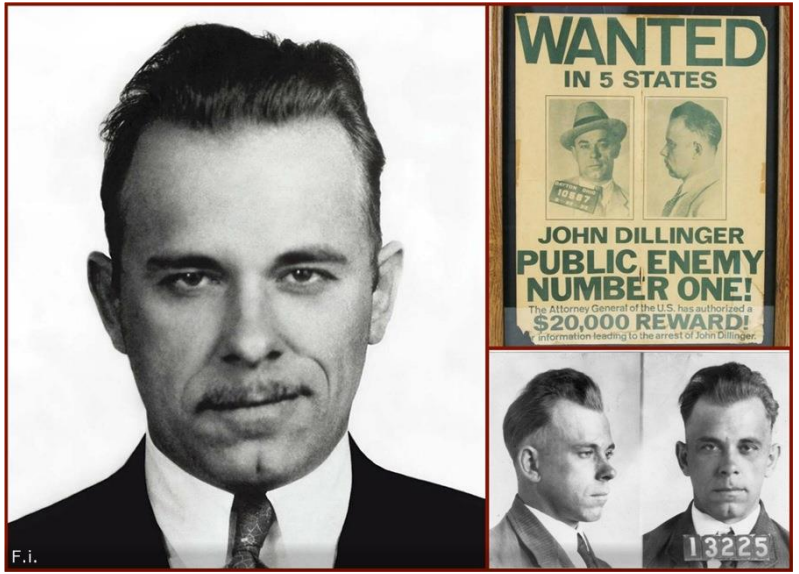
2015

2016

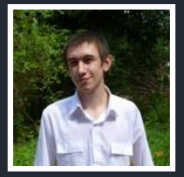
2017

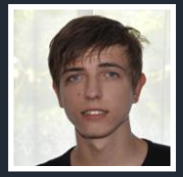
2018

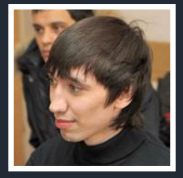
Нарушители в прошлом

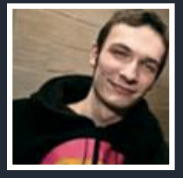


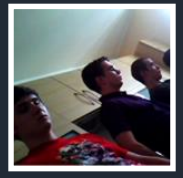
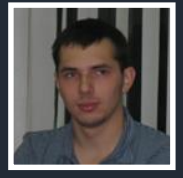
Нарушители в настоящем

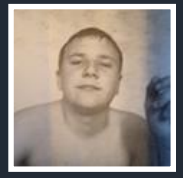







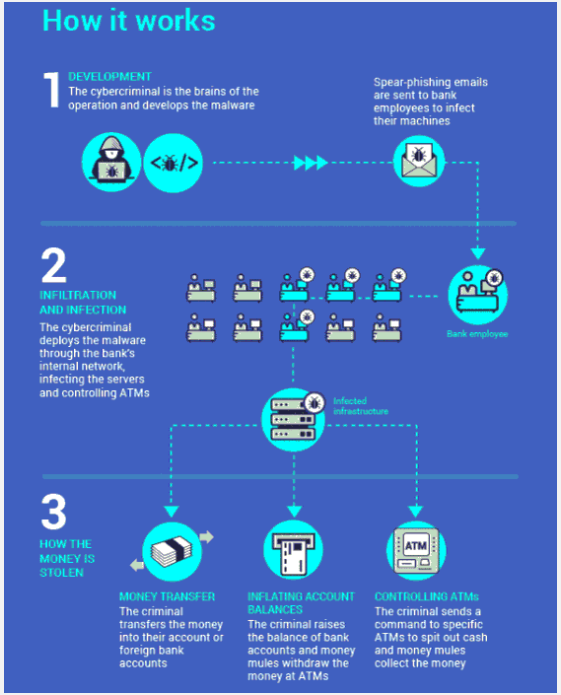



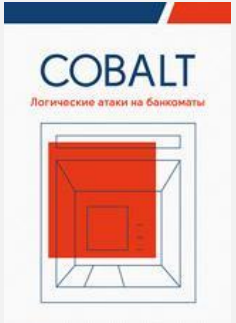

Пример схемы похищения денег

ТЕХНОЛОГИИ И МЕДИА, 26 МАР, 20:08 👁 29 271

В Испании задержан лидер хакеров — похитителей €1 млрд

В Испании задержан лидер хакерской группировки Cobalt, атаковавшей около сотни финансовых организаций в 40 странах. Общий ущерб от ее действий оценивается в €1 млрд. В Европоле заявили РБК, что он «из русскоязычного мира»





АО «ТЕЛЕКОМПАНИЯ НТВ» НАРУШИЛО ЗАКОН О РЕКЛАМЕ

ДОЧКА SAMSUNG ОПЛАТИЛА ШТРАФ В РАЗМЕРЕ 2,5 МЛН РУБЛЕЙ

«ЯНДЕКС» НАРУШИЛ ЗАКОН, РЕКЛАМИРУЯ БУКМЕКЕРОВ «1ХСТАВКА» И «LEON»

ОЧЕРЕДНОЙ ШТРАФ ЗА НЕНАДЛЕЖАЩУЮ РЕКЛАМУ В GOOGLE

https://fas.gov.ru

Центр реагирования CERT-GIB

CERT-GIB (Computer Emergency Response Team) — центр круглосуточного реагирования на инциденты информационной безопасности

- Мониторим появление фишинговых ресурсов, распространение вредоносного ПО, торговлю контрафактом
- Оказываем полную юридическую поддержку на всех этапах реагирования и расследования
- Немедленное реагирование на инциденты, в том числе с выездом на место преступления
- Оперативно блокируем опасные сайты в доменах .RU, .РФ, и еще более 1000 доменных зон
- Работаем по всему миру: через сеть партнеров, контакт с хостинг-провайдерами и регистраторами доменных имен
- Сбор, исследование и хранение цифровых доказательств
- Аутсорсинг мониторинга средств

Компетентная организация Координационного центра национального домена сети Интернет и Фонда развития интернета

Аккредитованный член международных сообществ FIRST и Trusted Introducer

Партнер IMPACT – международного партнерства по противодействию киберугрозам

Авторизован Университетом Карнеги, официально использует торговую марку CERT

Уникальная экспертиза

МНОГОЛЕТНИЙ ОПЫТ РАССЛЕДОВАНИЙ

Целевые атаки

Несанкционированный доступ

DDoS-атаки

Финансовые преступления

Корпоративные преступления

Крупнейшая в Восточной Европе Лаборатория компьютерной криминалистики и исследования вредоносного кода

Самое современное оборудование и ПО

Зарубежные и передовые отечественные продукты по компьютерной форензике, собственные разработки, в том числе позволяющие обойти технологии сокрытия следов

Поиск данных на любых типах носителей

Даже если они были удалены, скрыты или зашифрованы

Передовая вирусная аналитика

Более качественная, чем в антивирусных компаниях

Индивидуальный подход к расследованиям

Проектная команда из специалистов необходимого профиля: от E-Discovery и Forensic до экспертов в области финансового аудита и корпоративного права

Глубокое понимание экономики киберпреступлений

Восстановление цепочек движения денежных средств с помощью эксклюзивных разведданных Group-IB Threat Intelligence

Широкий круг партнеров в СНГ и зарубежных юрисдикциях,

включая Европол и Интерпол

Реагирование и криминалистика

24

круглосуточная поддержка профессиональной команды реагирования

Заключение по итогам реагирования:

- Откуда инициирован инцидент: изнутри или извне?
- Кем инициирован инцидент? Кто причастен к инциденту?
- Каковы объемы потерь и скомпрометированных данных?
- Каковы могут быть последствия для организации?
- Как предотвратить подобные инциденты?

Первичное реагирование

Подтверждение факта и определение типа инцидента

Выявление всех узлов сети, задействованных в инциденте

Конкретные рекомендации по устранению уязвимостей и оперативному восстановлению штатной работы IT-систем

Консультация службы безопасности и IT на предмет предотвращения рецидивов

Возможность выезда мобильной бригады на место инцидента

Сбор доказательств

Сбор всей необходимой информации об инциденте (в том числе из журналов регистрации событий, записей видеокамер, опроса сотрудников и др.)

Юридически безупречное оформление доказательств (упаковка и опечатывание носителей, документирование процесса сбора улик и пр.) для представления в суде, в т.ч. по искам третьих лиц

Проверка всей сети заказчика на предмет заражений

Расследование компьютерных преступлений

1000+

успешных расследований по всему миру

$300M

возвращено клиентам по итогам наших расследований

Помогаем правоохранительным органам в поиске и задержании убийц, воров и других преступников

РАССЛЕДУЕМ:

- Фишинг
- DoS/DDoS атаки
- Вымогательство
- Инсайдерские атаки
- Финансовые преступления
- Заражение вредоносным программным обеспечением
- Нарушение прав на объекты интеллектуальной собственности


Гражданин
Доверие
Сотрудниче
ство
Банки,
бизнес,
частный
сектор
Правоохран
ительные и
иные
государстве
нные органы

Спасибо за внимание!

Александр Сушко

Руководитель офиса, Group-IB

sushko@group-ib.by

+375297724963