АНАЛИТИЧЕСКАЯ РАЗВЕДКА

СТАТИСТИКА

66%

компаний стали жертвами экономических преступлений с начала 2018 г.

56%

компаний увеличили расходы на борьбу с экономическими преступлениями за последние 2 года

22%

компаний понесли ущерб свыше $1 млн от экономических преступлений

39%

доля руководителей среди внутренних правонарушителей в 2018 г. (15% – в 2016 г.)

** по данным исследования PwC в России за 2018 г.*

ТИПОВЫЕ УГРОЗЫ ДЛЯ БИЗНЕСА

01 Репутационные риски, «черный» PR

02 Санкционные и налоговые риски

03 Невыполнение контрагентом/клиентом договорных обязательств

04 Работа менеджмента и сотрудников против интересов компании

05 Ущерб из-за утечек информации, доступа к закрытым данным, использования вредоносного ПО

06 Мошенничество: присвоение и сокрытие активов, невозврат крупных кредитов, фишинг

АНАЛИТИЧЕСКАЯ РАЗВЕДКА: ПРЕДОТВРАЩЕНИЕ УГРОЗ

Информационно-аналитическая подготовка крупных сделок

Кадровая проверка ключевых сотрудников и руководителей

Предотвращение, выявление, содействие в расследовании хищений

Выявление «утечек» и поиск активов

Криминалистическое исследование компьютерных средств

Проведение судебной компьютерно-технической экспертизы

Участие IT-экспертов в процессуальных действиях

Аудит информационной безопасности

НАШИ МЕТОДИКИ

Аналитическая разведка

Компьютерная криминалистика

Социальная инженерия

Этичный хакинг

Также мы используем знания и методики подразделений собственной, информационной и экономической безопасности. Над задачей работают специалисты разных направлений, что и дает результат!

ЧТО ИСПОЛЬЗУЕМ

Внешние источники	Внутренние источники	Средства
Публичные сайты и сетевые СМИ	Почтовый архив	OSINT-инструменты
Социальные сети	Логи корпоративных систем	Собственные парсеры, базы, обработчики
Аккаунты и группы IM	Корпоративные мессенджеры	Аналитические системы и БД
Серверы раскрытия информации	Корпоративные БД	Pentest-инструменты
Доступные БД и реестры	Корпоративная телефония	Forensic-системы, оборудование
DarkNet, Tor, i2p	Корпоративные ПК	DLP-системы

ETHIC
EXTERNAL THREATS & HUMAN INTELLIGENCE CENTER

СЕРВИС ВЫЯВЛЕНИЯ УГРОЗ ДЛЯ БИЗНЕСА

УГРОЗЫ

Автоматический анализ источников вне периметра: от соцсетей до изолированной информации DarkNet

ОЦЕНКА

Аналитическая экспертиза уровня опасности для определения тактики реагирования на угрозы

ОПОВЕЩЕНИЕ

Отправка предупреждений об угрозах для бизнеса или инцидентах через специальный веб-портал

РЕАГИРОВАНИЕ

Блокировка источников, изменение технических настроек сервисов, проведение расследования

ПРИМЕР РАССЛЕДОВАНИЯ:

АРГЕНТИНСКИЕ ВАРРАНТЫ

ЗАДАЧА

Содействие при расследовании уголовного дела в отношении группы Урумова (махинации с аргентинскими варрантами и бонусами). Общий ущерб банковская группа «Открытие» оценила в $173 млн.

РАБОТЫ

- Выявление полной схемы мошенничества и новых фигурантов на основе телефонной детализации, анализа рабочей почты и движения ДС на счетах и других закрытых источников
- Поиск активов и счетов
- Выезды и снятие образов с цифровых носителей, их анализ и экспертиза

РЕЗУЛЬТАТЫ

- Бывший сотрудник группы «Открытие» Джордж Урумов лишен свободы на 12 лет
- Владимир Герсамия (Threadneedle Asset Management)лишен свободы на 7 лет
- Возвращены активы на сумму более $100 млн.

ПРИМЕР РАССЛЕДОВАНИЯ:

РАСТРАТА БЫВШИХ АКЦИОНЕРОВ

ЗАДАЧА

Содействие при расследовании уголовного дела в отношении топ-менеджеров банка «Траст». В 2012-2014 гг. руководство банка, действуя в интересах бывших акционеров, выдало кредиты фиктивным организациям на сумму 14,6 млрд. рублей.

РАБОТЫ

- Анализ родственных связей
- Анализ аффилированных юридических лиц
- Осмотры образов носителей
- Анализ рабочей переписки
- Мониторинг активности фигурантов
- Проверка деловых связей фигурантов

РЕЗУЛЬТАТЫ

- Лишены свободы директор казначейства (7 лет колонии) и финансовый директор (4 года)
- Заморожены активы бывших акционеров на сумму $830 млн
- Пресечены неоднократные попытки бывших топ-менеджеров продать имущество банка с использованием оригиналов документов, похищенных при увольнении

ПРИМЕР РАССЛЕДОВАНИЯ:

ХАКЕРСКАЯ АТАКА И ОБНАЛИЧИВАНИЕ

ЗАДАЧА

Расследование инцидента ИБ, раскрытие мошеннических схем, установление личностей руководителей и исполнителей. Используя уязвимости в банковском ПО, группа хакеров вывела на карточные счета и обналичила 330 млн рублей.

РАБОТЫ

- Анализ соцсетей фигурантов
- Анализ аффилированных юрлиц
- Выявление объявлений в даркнете о продаже кредитных карт
- Проведение технической экспертизы и анализа поведения хакеров
- Выявление скомпрометированных карт

РЕЗУЛЬТАТЫ

- Собраны все необходимые доказательства для судебного преследования
- Установлены дропы, вербовщики, дроповоды, обнальщики
- Выявлены и заблокированы счета-зомби, предназначенные для обналичивания и отмывания в будущем

НАШИ ПРЕИМУЩЕСТВА

Сертифицированные специалисты (пентесты, СКТЭ и др.)

Большой опыт раскрытия сложных схем хищений в крупных организациях

Работа со всеми возможными каналами: от соцсетей до собственных баз на несколько миллиардов объектов

Индивидуальный подход: покупаем или разрабатываем сами нужные средства, если этого требует задача

gk-is.ru