Group-IB

Intelligence
или как сохранить миллионы

2015

BOT-TREK

Примеры инцидентов в России

Хакеры похитили у Энергобанка около полумиллиарда рублей

27 февраля с 12:30 до 12:43 злоумышленники получили контроль над терминалом Энергобанка и провели на Московской бирже ряд несанкционированных операций по покупке и продаже валюты. В результате операций по невыгодному курсу банк потерял около 470 млн. рублей, часть из которых досталась неизвестным участникам торгов. Среди установленных лиц, получивших прибыль в результате этих операций, оказались клиенты брокерских компаний БКС, «Финам» и «Открытие».

Выставили на продажу переписку пресс-секретаря Медведева за 11 лет

Группировка «Анонимный интернационал» выложила в сеть несколько порций документов, которые были представлены как переписка сотрудников управления внутренней политики администрации президента России.
Кроме того, на продажу была выставлена переписка пресс-секретаря Дмитрия Медведева
Натальи Тимаковой. Источник в правительстве указывает, что был взломан почтовый ящик на закрытом домене gov.ru, который обслуживает ФСО.

Через «дыру» в Qiwi хакеры украли 90 млн руб.

Платежная система Qiwi сообщила в своем годовом отчете об обнаружении «бреши», которой воспользовались хакеры. В январе 2014 г. было взломано 687 аккаунтов пользователей Qiwi. Размер ущерба, зафиксированный компанией, составил 88 млн руб.

BOT-TREK

Примеры инцидентов

Home Depot's 56 Million Card Breach Bigger Than Target's

Home Depot Inc. said 56 million cards may have been compromised in a five-month attack on its payment terminals, making the breach much bigger than the holiday attack at Target Corp.

Chinese Hackers Target Israel's Iron Dome

Three Israeli defense contractors responsible for building the "Iron Dome" missile shield currently protecting Israel from a barrage of rocket attacks were compromised by hackers and robbed of huge quantities of sensitive documents pertain- ing to the shield technology.

SONY

Massive Sony breach sheds light on murky hacker universe

Last week Sony admitted to having suffered a major cybersecurity breach; hackers not only erased data from its systems, but also stole, and released to the public, pre-release movies, people's private informa- tion, and sensitive documents.

…Data Breach at Health Insurer Anthem Could Impact Millions, Banks: Card Thieves Hit White Lodging Again, FBI: Businesses Lost $215M to Email Scams, Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm, Sony Breach May Have Exposed Employee Healthcare, Salary Data, Malware Based Credit Card Breach at Kmart, Dairy Queen Confirms Breach at 395 Stores, Huge Data Leak at Largest U.S. Bond Insurer, Hackers Plundered Israeli Defense Firms that Built 'Iron Dome' Missile Defense System, eBay Urges Password Changes After Breach, Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen …

BOT-TREK

Целевые атаки 2014

Anunak	Взломано более 50 российских банков и 5 платежных систем, 16 ритейл-компаний. Доступ к изолированным банковским системам, банкоматам, электронной почте, платежным шлюзам.
Regin	Взломаны телеком-операторы, государственные компании, научно-исследовательские учреждения, политические организации. Доступ к конфиденциальной информации, слежение за GSM-сетями.
Energetic Bear	Взломаны энергетические, фармацевтические, строительные и образовательные учреждения.
Careto	Взломаны государственные, дипломатические, энергетические, нефтяные, инвестиционные компании и исследовательские институты.

BOT-TREK

Почему инциденты случаются

Средства защиты не дают сведений об атакующих, используемых инструментах, тактике проведения атак

случайно перехваченный пароль может стать началом целевой атаки

Невозможно выделить среди тысяч событий те, что имеют действительно важное значение

Без знаний о целях злоумышленников нельзя адекватно оценить важность события

Нет индикаторов, по которым можно выявить интересный инцидент

BOT-TREK

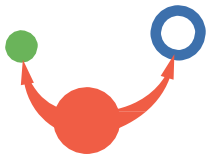
Что необходимо для проактивной защиты?

Intelligence

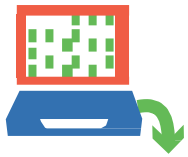
позволит предотвратить инцидент на этапе подготовки и стать проактивным

Постоянно участвовать в разборах разных инцидентов

Идентифицировать взломанные учетные записи в бот-сетях, фишинговые страницы



Отслеживать атаки на партнеров и клиентов



Отслеживать утечки данных уже за пределами периметра защиты

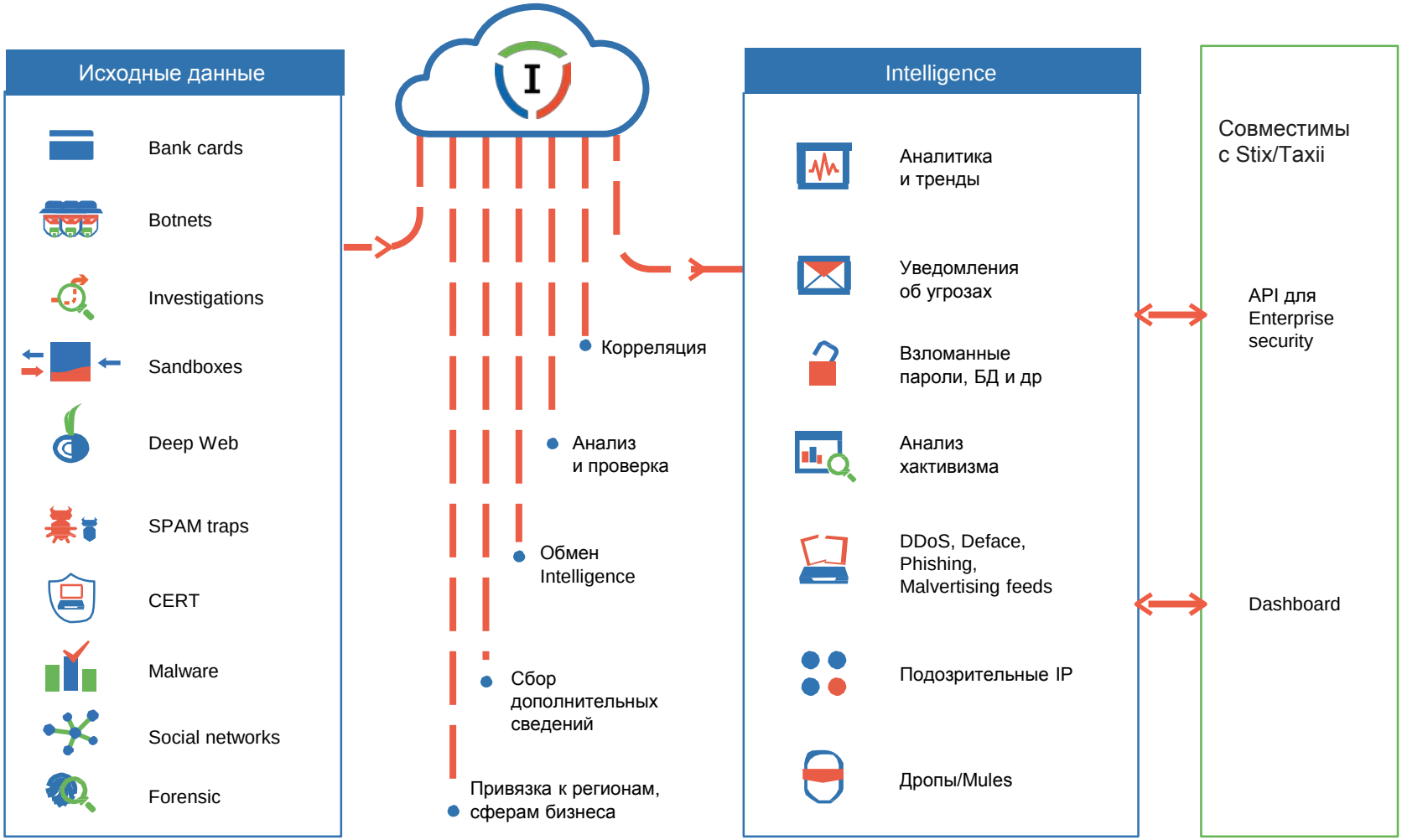
Иметь инфраструктуру для обработки данных и получения сведения о новых угрозах

Изучать данные о новых угрозах

Анализировать связи между событиями

BOT-TREK

Как работает Intelligence



Bot-Trek Intelligence

BOT-TREK

Какие данные предоставляются

Стратегические:

- Анализ действий преступных групп
- Оценки атак по странам/сегментам бизнеса
- Прогнозирование новых угроз
- Сведения о наиболее актуальных угрозах

Тактические/операционные:

- Сведения об угрозах и их анализ
- Сведения по текущим атакам
- Сведения о преступных группах, их инструментах/тактике
- Сведения о логинах/паролях компании, ее партнеров, клиентов

Технические индикаторы:

- IP и URL адреса
- Названия вредоносных вложений
- Темы писем с целевыми атаками
- Взломанные легитимные сайты, распространяющие вредоносные программы
- Изменения в операционной системе
- Аномальные признаки

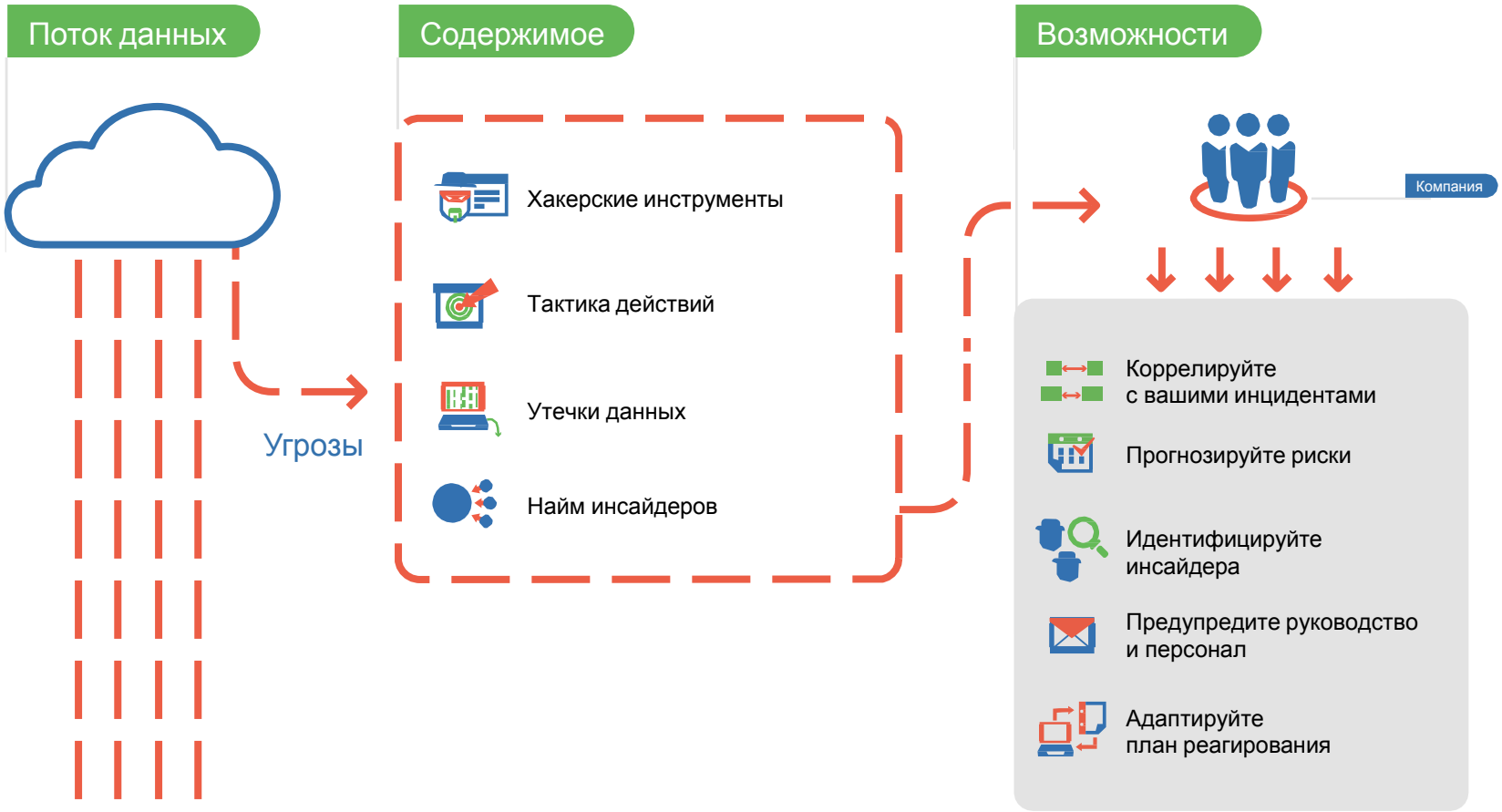
BOT-TREK

Скомпрометированные данные

Bot-Trek Intelligence

BOT-TREK

Угрозы



+7 (495) 984 33 64

www.group-ib.ru

info@group-ib.ru

facebook.com/groupib

youtube.com/groupib

twitter.com/groupib

linkedin.com/company/group-ib