ti.group-ib.ru

THREAT INTELLIGENCE

Мониторинг, анализ
и прогнозирование
угроз для компании,
клиентов и партнеров

Время для
предотвращения
будущих атак

Подробная
информация о
злоумышленниках

Усиление систем,
команды
и стратегии

ВЫСОКОТЕХНОЛОГИЧНАЯ СИСТЕМА МОНИТОРИНГА КИБЕРУГРОЗ

ОТ ЛУЧШИХ МИРОВЫХ ЭКСПЕРТОВ

Участвуя в расследованиях киберпреступлений с 2003 года, мы сформировали базу данных о злоумышленниках и высокотехнологичную систему слежения за ними. Наши эксперты узнают о будущих атаках на этапе подготовки инфраструктуры и заранее предупреждают клиентов Group-IB Threat Intelligence.

Group-IB входит в число лучших мировых поставщиков Threat Intelligence по версии Gartner, IDC, Forrester, Cyber Defense Magazine и SC Media

ОТВЕЧАЕТ НА КЛЮЧЕВЫЕ ВОПРОСЫ:

- Кто атакует вас, ваших клиентов, компании вашего сектора?
- Как и с помощью каких инструментов проводятся атаки?
- Кто из ваших клиентов и сотрудников уже стал жертвой киберпреступников?
- Что говорят о вашей компании на хакерских площадках?
- Как преступники используют или планируют использовать ваш бренд?

КОМАНДА ПРОФЕССИОНАЛОВ

Эксперты Group-IB первыми узнают о новых атаках и участвуют в реагировании на инциденты, обогащая технологический стек знаниями о новых тактиках и инструментах злоумышленников

15 ЛЕТНИЙ ОПЫТ

анализа угроз и расследования инцидентов

> Расследование особо сложных высокотехнологичных преступлений позволяет Group-IB получать эксклюзивную информацию о киберпреступниках, их взаимосвязях и другие разведданные.
>
> **Gartner**

УНИКАЛЬНЫЕ ИСТОЧНИКИ

Threat Data Intelligence

Исследования C&C серверов мобильных и ПК-ботнетов, кардшопы, сенсоры на уровне интернет-провайдеров

Malware Intelligence

Сетевые датчики и песочницы, распределенная сеть мониторинга и ловушек HoneyNet, Sinkhole, спам-ловушки

Собственная «песочница» глубокого анализа вредоносных файлов — TDS Polygon

Human Intelligence

Многолетняя практика реагирования на инциденты и расследования киберпреступлений, мониторинг закрытых сообществ

СОБСТВЕННЫЕ ТЕХНОЛОГИИ

Автоматизированная система поиска и извлечения данных

- Проактивное обнаружение фишинга и извлечение фишинг-наборов
- Извлечение конфигурационных файлов вредоносных программ
- Сбор и анализ данных с закрытых хакерских форумов на 11 языках

Анализ данных с фокусом на атакующих

- Отслеживание изменений в инструментах злоумышленников
- Составление профилей злоумышленников
- Машинное обучение для оперативной корреляции больших массивов данных

Правила выявления инфраструктуры для будущих атак
основаны на уникальных поведенческих характеристиках злоумышленников

4,2 МЛРД
IP-адресов
+ исторические данные за 2 года

650 МЛН
доменов
+ исторические данные за 15 лет

689 МЛН
SSL-сертификатов

145 МЛН
SSH-ключей

THREAT INTELLIGENCE ЗАЩИЩАЕТ ОТ КЛЮЧЕВЫХ КИБЕРУГРОЗ

Целевые атаки

Выявляйте новые угрозы и будьте в курсе активности группировок киберпреступников
Уведомления об угрозах содержат оценку надежности, индикаторы компрометации, описание техники в MITRE's ATT&CK и практические рекомендации по реагированию.

100 000+

профилей злоумышленников

и значимые данные об активности киберпреступников, готовящих атаки на вашу компанию или индустрию.

Фишинговые атаки

Собственная технология автоматического обнаружения и блокировки фишинга позволяет оперативно остановить атаку, а извлечение адресов электронной почты, используемых для сбора данных, — лишить злоумышленников доступа к украденой информации.

Незаконное использование бренда

Вы будете оперативно узнавать о появлении поддельных доменов, рекламных сообщений, SSL-сертификатов и мобильных приложений.

Утечки данных

Узнавайте о компрометации данных на ранней стадии
Мониторинг инфраструктуры киберпреступников позволяет выявить утечку данных на ранних стадиях. Вы узнаете о скомпрометированных аккаунтах, счетах, банковских картах и мобильных устройствах до того, как они будут выставлены на продажу на хакерских форумах.

ГДЕ, КОГДА И КАК —

расширенный контекст компрометации позволяет быстро ликвидировать источник угрозы.

УСИЛЬТЕ КОМАНДУ, ИНФРАСТРУКТУРУ И СТРАТЕГИЮ

Увеличьте эффективность используемых вами систем безопасности

Уникальные данные, обогащенные контекстом...

Скомпрометированные аккаунты, банковские карты и мобильные устройства
Фишинговые атаки
Целевые атаки
Утечки данных

... а также технические индикаторы

- Нарушения бренда
- Уязвимости
- Дефейсы
- DDoS-атаки
- Мулы
- Открытые прокси
- SOCKS прокси на ботах
- Хактивизм
- Подозрительные IP
- Узлы Tor

Удобная интеграция через API, STIX/TAXII

- SIEM
- Firewall
- TIPS
- IDS/IPS

Усильте свою команду персональным аналитиком

В любой момент вы можете обратиться за дополнительным индивидуальным исследованием: сбором индикаторов, профайлингом атакующих, исследованием подозрительной активности на хосте и т.д.

ДО 300 ЧАСОВ

поддержки персонального аналитика в год включено в пакеты подписки

Совершенствуйте стратегию на основании надежной информации

Выберите правильные решения для защиты и максимизируйте ROI благодаря проверенной информации об изменениях ландшафта киберугроз.

ЕЖЕМЕСЯЧНЫЕ, КВАРТАЛЬНЫЕ И ГОДОВЫЕ ОТЧЕТЫ

о тенденциях киберпреступлений создаются вручную опытными экспертами

Все данные доступны через удобный веб-интерфейс

ГОТОВАЯ ИНТЕГРАЦИЯ С THREAT INTELLIGENCE ПЛАТФОРМАМИ

THREATCONNECT ANOMALI eclectic iq THREATQUOTIENT

Group-IB – один из ведущих мировых разработчиков решений для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети

15 лет
ПРАКТИЧЕСКОГО ОПЫТА

55 000+
ЧАСОВ РЕАГИРОВАНИЯ

1 000+
РАССЛЕДОВАНИЙ ПО ВСЕМУ МИРУ

300+
СПЕЦИАЛИСТОВ И РАЗРАБОТЧИКОВ

Официальный партнер

INTERPOL EUROPOL

Group-IB входит в число лучших мировых поставщиков Threat Intelligence по версии Gartner, IDC, Forrester, Cyber Defense Magazine и SC Media.

Эксперты Group-IB проводили тренинги профессионального развития для специалистов Europol, INTERPOL, правоохранительных органов, корпоративных команд безопасности и преподавателей университетов в Великобритании, Германии, Нидерландах, Бельгии, Франции, Таиланде, Бахрейне и Ливане.

УЗНАТЬ БОЛЬШЕ

о возможностях Threat Intelligence

tds.group-ib.ru

СВЯЖИТЕСЬ С НАМИ

Чтобы провести тест-драйв TDS

tds@group-ib.ru

ПОЗНАКОМЬТЕСЬ С GROUP-IB

group-ib.ru
facebook.com/GroupIB

СЕРВИСЫ GROUP-IB

Укрепите кибербезопасность с помощью опытных специалистов, погруженных в реагирование и расследование актуальных атак и имеющих доступ к одной из самых современных систем слежения за киберугрозами в мире.

АУДИТ И ОЦЕНКА РИСКОВ

- Тестирование на проникновение
- Исследование уязвимостей
- Анализ исходного кода
- Compromise Assessment
- Red Teaming
- Pre-IR Assessment
- Оценка соответствия

THREAT HUNTING И РЕАГИРОВАНИЕ

- Managed Threat Hunting
- APT-мониторинг
- Криминалистическое реагирование (целевые атаки, утечки и др.)
- Оперативное реагирование (фишинг, DDoS, нарушение прав на интеллектуальную собственность и др.)
- Реагирование «по подписке»

КРИМИНАЛИСТИКА

- Сбор цифровых доказательств
- Криминалистический анализ
- Анализ вредоносного кода

РАССЛЕДОВАНИЯ

- Целевые атаки
- Инциденты информационной безопасности
- Финансовые и корпоративные преступления