СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

Secure Portal

ВЫЯВЛЕНИЕ МОШЕННИЧЕСТВ НА ЭТАПЕ ПОДГОТОВКИ

Без установки дополнительного программного обеспечения на устройства клиентов Secure Portal в режиме реального времени выявляет:

- несанкционированный доступ к личным кабинетам и персональным данным
- сбор данных о платежных картах и использование ворованных карт
- взлом бонусных счетов
- хищение инвентаря в онлайн-играх
- использование ботов (для подбора паролей, накрутки голосов, размещения отзывов)
- показ предложений конкурентов на страницах портала
- совместное использование платной подписки

и другие схемы мошенничества.

Рост пользовательской базы портала автоматически увеличивает риски мошенничества, бенефициарами которого могут быть как киберпреступники, так и ваши конкуренты.

Используя данные из уникальных источников, технологию device fingerprinting и собственные решения на базе машинного интеллекта, Secure Portal позволяет предотвратить ущерб, детектируя признаки подготовки преступной схемы в момент захода пользователя на ваш сайт.

Сохраняет ваши деньги

Снижает объем возмещений (chargeback) денежных средств после оплаты ворованными картами

Снижает ущерб от бонусного мошенничества

Сокращает издержки на обработку претензий клиентов

Укрепляет вашу репутацию

Предотвращает утечки персональных данных и другой конфиденциальной информации

Укрепляет доверие к бренду, давая возможность предупреждать клиентов о попытках мошенничества

Снижает репутационные риски

КОМУ ПОЛЕЗЕН SECURE PORTAL

- Интернет-магазины
- E-commerce сервисы
- Порталы госуслуг
- Сайты с платным контентом
- Игровые порталы
- Корпоративные порталы

УНИКАЛЬНЫЕ ИСТОЧНИКИ ДАННЫХ ОБ УГРОЗАХ

Высокотехнологичная инфраструктура сбора данных об активности киберпреступников дает нам возможность следить за появлением новых тактик мошенничества и оперативно обновлять маркеры подготовки преступных схем.

КИБЕРРАЗВЕДКА

Сведения о скомпрометированных банковских картах и учетных записях позволяют предотвращать их использование злоумышленниками, а ежедневно обновляющиеся данные о TOR-узлах, SOCKS-proxy и других подозрительных IP дают возможность быстрее детектировать мошенническую активность.

КРИМИНАЛИСТИКА

Заключения Лаборатории компьютерной криминалистики и исследования вредоносного кода позволяют с высокой точностью устанавливать признаки работы новых программ, используемых для реализации мошеннических схем.

МАШИННЫЙ ИНТЕЛЛЕКТ

Обрабатывая большой объем данных о поведении клиентов, машины выявляют отклонения и другие аномалии. Аналитики Group-IB выделяют те из них, которые могут свидетельствовать о подготовке и реализации преступной схемы, обучая машины находить ранее неизвестные маркеры мошеннических схем.

2 место

в мире занимает Россия по числу утечек конфиденциальных данных

КАК РАБОТАЕТ SECURE PORTAL

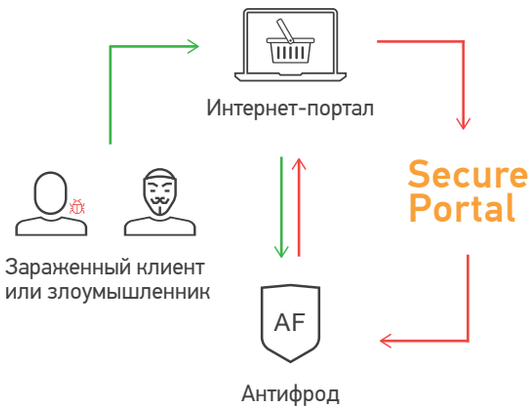
СБОР ДАННЫХ

JavaScript-модуль Secure Portal загружается вместе со страницами банка. Работая незаметно для клиента, модуль:

контролирует отсутствие инъекций на страницы портала,

собирает идентификационные данные клиентского устройства и другие сведения, которые помогают выявить мошенничества,

передает данные в серверную инфраструктуру Group-IB по защищенному каналу.



Работа скрипта не сказывается на скорости загрузки страниц.

ОБРАБОТКА ДАННЫХ

Для корреляции и классификации полученных данных используются данные из уникальных источников.

В случае выявления фактов мошенничества, Group-IB незамедлительно информирует вас о них.

API для интеграции с системами безопасности портала позволяет настраивать уведомления и запускать процедуры реагирования по отработанным схемам в режиме реального времени.

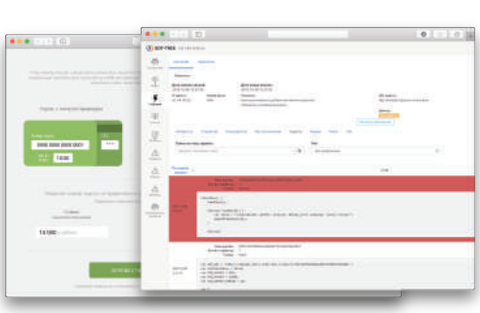
SECURE PORTAL ПОМОЖЕТ ЗАЩИТИТЬ ВАШ БРЕНД

Для хищения учетных записей и данных банковских карт мошенники создают поддельные сайты портала. Многие из них просто делают копию сайта.

Если код оригинального сайта содержит модуль Secure Portal, при заходе первого пользователя на мошенническую копию, модуль сообщит доменное имя этого сайта.

Мы передадим доменное имя Центру круглосуточного реагирования CERT-GIB, который, после вашего подтверждения, оперативно заблокирует фишинговый ресурс.

МАКСИМАЛЬНОЕ УДОБСТВО ИСПОЛЬЗОВАНИЯ



Веб-интерфейс позволяет ознакомиться с подробной информацией о каждой подозрительной сессии.

Сверхбыстрое внедрение

Внедрение модуля Secure Portal в код сайта занимает не больше 20 минут.

Облачный интерфейс

Вся информация о подозрительных сессиях доступна в веб-интерфейсе, через который удобно отслеживать уведомления в течение дня.

Документированное API

Комфортная интеграция с системами безопасности и IT-инфраструктурой портала.

Аналитическая поддержка

Консультации опытных специалистов, основанные на данных постоянно пополняемой базы знаний Group-IB.

СВЯЖИТЕСЬ С НАМИ
чтобы провести
тест-драйв Secure Portal
+7 (495) 984 33 64
sp@group-ib.ru

УЗНАЙТЕ БОЛЬШЕ
о возможностях предотвращения хищений с помощью Secure Portal
sp.group-ib.ru

ПОЗНАКОМЬТЕСЬ С GROUP-IB
– одним из 7 лучших поставщиков данных киберразведки (threat intelligence) в мире по версии Gartner
www.group-ib.ru