СИСТЕМА РАННЕГО ПРЕДУПРЕЖДЕНИЯ КИБЕРУГРОЗ

Secure Bank

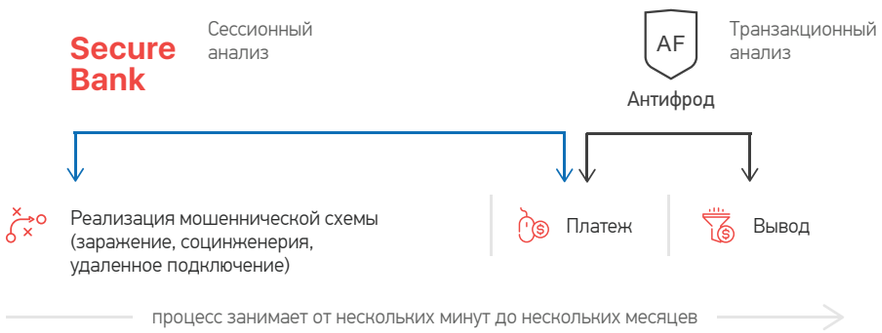
ВЫЯВЛЕНИЕ ХИЩЕНИЙ НА ЭТАПЕ ПОДГОТОВКИ

Без установки дополнительного программного обеспечения на устройства клиентов Secure Bank в режиме реального времени выявляет подготовку и проведение хищений денежных средств с использованием следующих инструментов:

- внедрение зловредных инъекций на страницы интернет-банкинга
- фишинговые атаки и приемы социальной инженерии
- несанкционированные удаленные подключения к устройствам клиента и проведение транзакций от его имени
- банковские трояны с функцией автоматического создания платежа или подмены реквизитов
- проникновение через 0-day уязвимости
- новые версии вредоносного кода

Современные инструменты киберпреступников (удаленные подключения, веб-инжекты для «автозалива», трояны, позволяющие перехватывать SMS) делают традиционные средства защиты от фрода на стороне клиента неэффективными.

Классический антифрод на стороне банка не видит признаков подготовки к хищению на устройстве клиента, срабатывает после приема мошеннического платежа и оставляет мало времени на принятие решения.



Secure Bank устраняет «слепые пятна» в обеспечении безопасности онлайн-платежей, выявляя различные признаки подготовки хищения при попытке авторизации в интернет-банке.

Сохраняет ваши деньги

Предотвращает хищения за счет раннего детектирования мошенничеств

Не требует инвестиций в масштабирование на всю клиентскую базу

Сокращает издержки на обработку ложных срабатываний и звонки клиентам

Укрепляет вашу репутацию

Повышает защищенность и привлекательность ваших систем онлайн-банкинга

Укрепляет доверие к банку, давая возможность предупреждать клиентов о заражениях и атаках

Снижает репутационные риски

УНИКАЛЬНЫЕ ИСТОЧНИКИ ДАННЫХ ОБ УГРОЗАХ

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

КИБЕРРАЗВЕДКА

Сведения о скомпрометированных учетных записях позволяют предотвращать хищения не только у клиентов, чьи устройства были заражены, но и у тех, чьи идентификаторы были перехвачены хакерами в результате фишинговой атаки.

КРИМИНАЛИСТИКА

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

МАШИННЫЙ ИНТЕЛЛЕКТ

Машинный анализ большого объема данных о поведении клиентов позволяет выявить отклонения и другие аномалии. Аналитики Group-IB выделяют те из них, которые могут свидетельствовать о компрометации устройства, обучая машины находить ранее неизвестные маркеры подготовки мошеннических операций.

Результаты работы Secure Bank доступны в облачном интерфейсе.

КАК РАБОТАЕТ SECURE BANK

СБОР ДАННЫХ

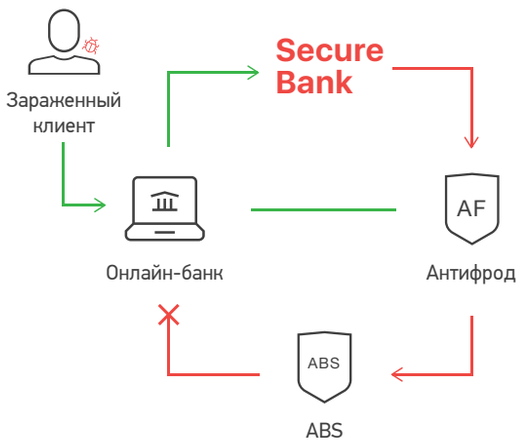
JavaScript-модуль Secure Bank загружается вместе со страницами банка. Работая незаметно для клиента, модуль:

контролирует отсутствие инъекций на страницы интернет-банка,

собирает идентификационные данные клиентского устройства

выявляет различные признаки работы вредоносных программ

передает данные в северную инфрастуктуру Group-IB по защищенному каналу.



Работа скрипта не сказывается на скорости загрузки страницы. Передача данных, составляющих банковскую тайну, не производится.

ОБРАБОТКА ДАННЫХ

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

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

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

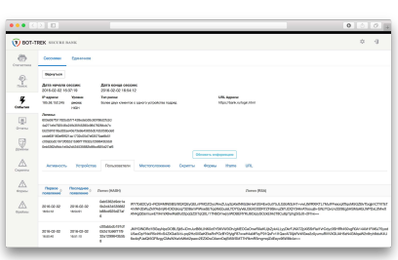
SECURE BANK ПОМОЖЕТ ЗАЩИТИТЬ ВАШ БРЕНД

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

Если код оригинального сайта содержит модуль Secure Bank, 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.

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-инфрастуктурой банка.

Наглядные отчеты

Визуализированная статистика по периодам и по типам событий позволяет отслеживать изменения в динамике и характере угроз.

Аналитическая поддержка

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

ГОТОВАЯ ИНТЕГРАЦИЯ С ИНФРАСТРУКТУРОЙ БАНКА:

ДБО

BSS

R-Style Softlab

Антифрод

SAS

FRAUDWALL

RSA

Intellinx Insider Threat Intelligence

SIEM

QRadar

ArcSight An HP Company

WAF

POSITIVE TECHNOLOGIES

СВЯЖИТЕСЬ С НАМИ
чтобы провести тест-драйв Secure Bank
+7 495 984 33 64
sb@group-ib.ru

УЗНАЙТЕ БОЛЬШЕ
о возможностях предотвращения хищений с помощью Secure Bank
sb.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