KASPERSKY lab

KASPERSKY FRAUD PREVENTION FOR ENDPOINTS

www.kaspersky.ru

KASPERSKY FRAUD PREVENTION

1. Способы атак на системы онлайн-банкинга

Главным мотивом совершения киберпреступлений является финансовая выгода. Современные преступные группировки, имеющие сложную структуру, пользуются разнообразными приемами для похищения денег через интернет-банки и сайты финансовых услуг. Это может быть как вмешательство с помощью вредоносного ПО в санкционированные транзакции с целью перевода денег на счета злоумышленников, так и сочетание фишинга с приемами социальной инженерии для получения незаконного доступа к счетам пользователей.

Можно выделить две основные угрозы:

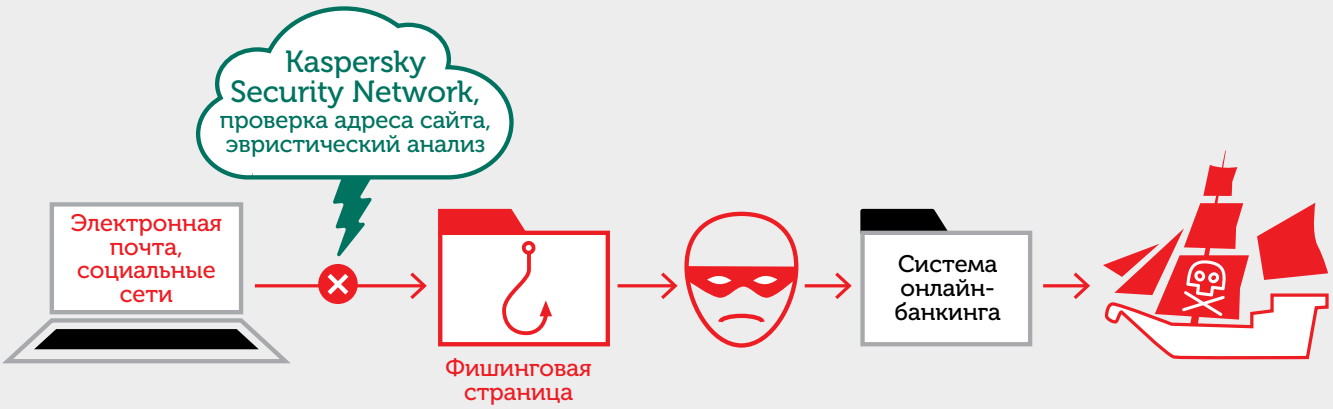
- **Захват банковского счета** – кража учетных данных пользователя и перевод денег со счета с использованием этих данных
- **Вмешательство в транзакции** – изменение параметров транзакции или создание новой транзакции от имени клиента

Для достижения своих целей киберпреступники применяют сочетание различных приемов, среди которых:

- кража учетных данных
- фишинг
- модификация веб-страниц (веб-инжекты)
- перехват данных, вводимых в веб-формы
- перехват данных, вводимых с клавиатуры
- кража данных посредством создания снимков экрана
- атаки с подменой ресурсов (серверов и пр.)
- вмешательство в транзакции
- атаки «человек посередине» (Man-in-the-Middle)
- атаки посредством удаленного доступа
- атаки «человек в браузере» (Man-in-the-Browser)

2. Защита от мошенничества

2.1 Обнаружение и удаление вредоносного ПО



Kaspersky Fraud Prevention защищает операции онлайн-банкинга, даже если на компьютере пользователя уже присутствует вредоносное ПО. Сразу после установки Kaspersky Fraud Prevention выполняет проверку системы на наличие вредоносного ПО для финансовых систем. Пользователь получает сообщение об обнаруженных проблемах с предложением удалить вредоносные файлы и вылечить компьютер. Далее решение выполняет проверку каждый раз, когда запускается защищенный браузер для банкинга.

ПРИМЕР ИЗ ПРАКТИКИ

Крупный российский банк подвергся атаке вредоносного ПО, которое автоматически перенаправляло клиентов банка на фишинговую страницу. В результате перенаправления пользователи лишались возможности попасть на настоящий сайт банка, а попав на поддельную страницу, передавали свои учетные данные банкинга киберпреступникам. Решение Kaspersky Fraud Prevention успешно удалило вредоносное ПО с компьютеров клиентов банка и обеспечило им возможность безопасно совершать банковские операции в будущем.

Kaspersky Fraud Prevention for Endpoints предназначен специально для поиска банковского вредоносного ПО. Решение совместимо со всеми популярными антивирусными программами и может использоваться вместе с традиционным антивирусным решением.

2.2 Защита канала связи с банком

Kaspersky Fraud Prevention не просто превращает компьютер пользователя в безопасную среду для выполнения операций онлайн-банкинга и проверяет подлинность открываемого банковского ресурса, но также обеспечивает защиту интернет-канала, связывающего банк с клиентами.

Каждый раз, когда пользователь начинает сеанс онлайн-банкинга, Kaspersky Fraud Prevention проверяет сертификат безопасности веб-сайта, сравнивая его с эталонным сертификатом, хранящимся в облачной среде Kaspersky Security Network. Такая проверка защищает от атак «человек посередине» и атак с подменой DNS-серверов и прокси-серверов.

Если решение обнаруживает подозрительный сертификат, система оповещает об этом пользователя.

2.3 Защита от угроз в браузере

2.3.1 АТАКИ С УДАЛЕННЫМ УПРАВЛЕНИЕМ БРАУЗЕРОМ

Kaspersky Fraud Prevention for Endpoints обеспечивает защиту от удаленного управления браузером посредством оконных сообщений Windows, не позволяя посторонним получать удаленный доступ.

2.3.2 АТАКИ С ВНЕДРЕНИЕМ КОДА

Защита от загрузки недоверенных модулей в процесс браузера с проверкой сигнатур DLL по локальной базе и в облаке (KSN).

2.3.3 ЗАЩИТА ОТ СНЯТИЯ СКРИНШОТОВ

Защита от создания снимков экрана блокирует многочисленные технологии, используемые злоумышленниками, чтобы делать снимки окна, открытого в браузере.

2.3.4 ПОИСК УЯЗВИМОСТЕЙ В ОС

Специальная обновляемая база уязвимостей, по которой проводятся проверки:

- ОС на наличие последних обновлений
- памяти ядра на наличие уязвимостей

2.3.5 БЕЗОПАСНАЯ КЛАВИАТУРА

При использовании защищенного браузера Kaspersky Fraud Prevention for Endpoints защищает все поля ввода. Решение отслеживает и обрабатывает все нажатия клавиш через собственный драйвер клавиатуры и исключает перехват вводимых данных вредоносными программами. Защищенной клавиатурой можно пользоваться как в безопасном браузере, так и в обычных окнах браузера.

2.3.6 ЗАЩИТА БУФЕРА ОБМЕНА

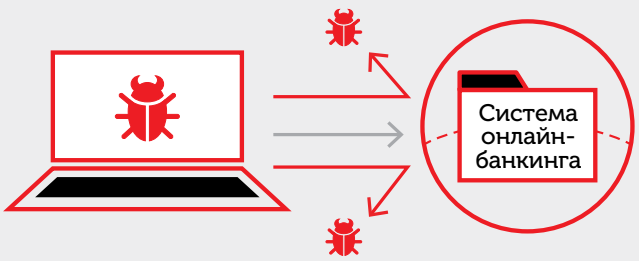
Запрещает недоверенным приложениям доступ к буферу обмена.

2.3.7 САМОЗАЩИТА

Защищает компоненты Kaspersky Fraud Prevention for Endpoints:

- разделы реестра Windows
- файлы
- процессы
- потоки

2.4 Анти-фишинг в браузере



В системе «Лаборатории Касперского» для защиты от фишинга традиционные локальные базы сочетаются с эвристическими и облачными технологиями, что позволяет эффективно блокировать даже новейшие, неизвестные ранее угрозы.

Постоянно обновляемый облачный модуль анти-фишинга содержит маски фишинговых ссылок. Новые угрозы добавляются в облачную базу в течение нескольких секунд после их обнаружения, что обеспечивает защиту пользователей от фишинговых сайтов, адреса которых еще не попали в локальные базы.

В обширной локальной базе анти-фишинга, хранящейся на устройствах пользователей, содержатся все наиболее распространенные маски фишинговых ссылок. Когда пользователь переходит по URL-адресу, которого нет в локальной базе, система автоматически проверяет его по облачной базе.

Когда пользователь нажимает на ссылку, ведущую на фишинговую веб-страницу, еще не попавшую в базы «Лаборатории Касперского», защита осуществляется эвристическим веб-компонентом системы анти-фишинга.

3. Консоль Kaspersky Fraud Prevention

Решение Kaspersky Fraud Prevention for Endpoints имеет удобную единую консоль управления. Она открывает доступ к обезличенным данным о пользователе, его устройстве и сеансе онлайн-банкинга, необходимым для уникальной идентификации.

3.1 Панель отчетов

Консоль управления Kaspersky Fraud Prevention for Endpoints предоставляет информацию о компьютере пользователя, сеансах онлайн-банкинга, операционной системе и установленном ПО, а также обо всех имевших место атаках: фишинговых, «человек посередине» (Man-in-the-Middle), «человек в браузере» (Man-in-the-Browser) и др.

3.2 Удаленная настройка Kaspersky Fraud Prevention for Endpoints

Консоль позволяет удаленно менять параметры Kaspersky Fraud Prevention for Endpoints.

3.3 Статистика

Консоль также позволяет передавать статистику во внутренние системы банка (например, системы мониторинга транзакций), чтобы повысить уровень обнаружения угроз и снизить вероятность ложноположительных срабатываний.

4. Порядок внедрения

Интеграция обычно проводится в 3 этапа.

1. Настройка решения в соответствии с требованиями банка для создания сервиса онлайн-банкинга по индивидуальному проекту. «Лаборатория Касперского» поддерживает модель работы под брендом клиента, и на странице банкинга может использоваться привычный фирменный стиль банка, включая логотипы, цветовые схемы, шрифты и особенности компоновки. Значки на рабочем столе и в области уведомлений также можно настроить в соответствии с требованиями банка.

2. Интеграция с внутренними системами банка. Kaspersky Fraud Prevention for Endpoints позволяет получать данные о версии и состоянии продукта при подключении к онлайн-банкингу. Для этого используется специальный скрипт, описанный в документации. Мы рекомендуем три основных рабочих сценария, но каждый банк может выбрать собственный способ использования полученных данных.

3. Затем банк может выбрать порядок распространения приложения среди своих клиентов. Например, можно проверить, установлено ли на компьютерах пользователей решение Kaspersky Fraud Prevention, и в случае необходимости предложить им его загрузить. Банк может выбрать и другой способ распространения приложения. С целью экономии вычислительных ресурсов банка приложение в основном размещается на серверах «Лаборатории Касперского» и доступно через загрузчик (размером 2 МБ), который передается банку на этапе внедрения.

4. Процесс установки обычно занимает около двух недель. Выделенная группа специалистов «Лаборатории Касперского» помогает встроить решение в инфраструктуру банка и устранить все возникшие проблемы.

Узнать больше: www.kaspersky.ru/business-security/fraud-prevention