kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Fraud Prevention

Проактивная защита от мошенничества с учетной записью

Стремительное развитие векторов атак говорит о необходимости кросс-канального подхода к обеспечению безопасности и защите личного кабинета пользователя.

Клиентские устройства, которые вы не контролируете, находятся за пределами вашего периметра безопасности и, скорее всего, недостаточно или вовсе не защищены. Несмотря на это, клиенты регулярно получают доступ для дистанционной работы с вашими услугами и таким образом постоянно находятся в зоне риска. А поскольку они подключаются к личному кабинету и из браузера, и из мобильного приложения, и с разных устройств на разных платформах, это делает вопрос безопасности личного кабинета особенно актуальным.

Кроме того, мошенники часто атакуют один канал, чтобы обеспечить кросс-канальный фрод (например, получая доступ к недостаточно защищенным данным для входа в мобильное приложение, они атакуют онлайн-кабинет для захвата учетной записи). Это приводит к очевидному выводу: формировать стратегию защиты необходимо комплексно, принимая во внимание личный кабинет пользователя, а не только устройство или один из каналов.

О решении

Kaspersky Fraud Prevention Cloud:

- Анализирует комбинацию параметров и событий со всех устройств пользователя, использующихся для входа в личный кабинет.
- Принимает решения на основании общей репутации устройств и личных кабинетов.
- Позволяет эффективно обнаруживать сложные атаки на уровне личного кабинета пользователя

Kaspersky Fraud Prevention Cloud способен обнаруживать атаки, направленные как на личный кабинет, так и на банковскую сессию, такие как:

- захват учетной записи (ATO)
- мошенничество с созданием новой учетной записи (NAF)
- фишинг, фарминг, смишинг
- автоматизированные средства: боты, валидация карт, перекрестная проверка учетных данных
- атаки с использованием средств удаленного администрирования (RAT)
- атаки «Man-in-the-Browser»

Кросс-канальный подход к безопасности

Ключевые технологии

Kaspersky Fraud Prevention Cloud объединяет в себе четыре ключевые технологии предотвращения мошенничества, основанные на алгоритмах машинного обучения:

Безагентное обнаружение вредоносных программ. Проверяет, заражено ли устройство вредоносным ПО, без установки каких-либо программ на стороне пользователя. Эти данные используются для Аутентификации на основе риска и поведенческого моделирования при помощи машинного обучения, а также для определения легитимности транзакций.

Поведенческий анализ. Исследует поведение пользователя во время сессии и в момент входа в личный кабинет. Также рассматриваются типичные элементы навигации, временные показатели и другие аспекты поведения. Это позволяет сформировать профиль нормального, легитимного поведения и на ранней стадии выявлять любую аномальную или подозрительную активность.

Поведенческая биометрия. Анализирует различные виды взаимодействия пользователя с устройством, такие как движения мыши, нажатия, скроллы, прикосновения, движения по экрану устройства и т. д., чтобы определить, используется ли это устройство реальным пользователем. Эта технология позволяет выявлять ботов и средства удаленного администрирования.

Анализ устройства и окружения. Использует данные облачной репутационной сети Kaspersky Security Network, чтобы идентифицировать «хорошие» устройства и использовать эти данные для аутентификации пользователя. На основании глобальной репутации устройств, IP-адресов, геолокационных показателей и других данных любой атрибут, некогда вовлеченный в мошеннические действия, проактивно обнаруживается и отображается как подозрительный или относящийся к фроду.

Методы машинного обучения

Являясь ключевой частью системы, усиливают используемые технологии, открывая доступ к дополнительным компонентам определения мошенничества:

Аутентификация на основе риска (RBA) делает возможным динамическую оценку уровня риска в момент входа пользователя в систему. На основе этой оценки и вердиктов, которые в реальном времени формирует Kaspersky Fraud Prevention Cloud, ваша организация может принять решение о том, как следует обрабатывать ту или иную транзакцию или событие: предоставить доступ, запросить дополнительную аутентификационную информацию или ограничить доступ к сервисам. Это позволяет обнаруживать фрод еще эффективнее и реагировать на попытки мошенничества в режиме реального времени. В то же время легитимные пользователи входят в систему, минуя дополнительные шаги аутентификации.

Непрерывная оценка аномалий предоставляет постоянную оценку риска сессии, основываясь на анализе поведения, устройства и окружения, биометрических показателях и другой информации. Это значительно повышает эффективность внутренних систем мониторинга, предоставляя средство раннего обнаружения и автоматизации, а также увеличивая показатели детектирования. Рискованные транзакции могут стать объектом особого внимания и ручной обработки, в то время как легитимные могут обрабатываться автоматически, без каких-либо задержек.

Kaspersky Fraud Prevention Cloud не заменяет ваше текущее решение по мониторингу транзакций, а дополняет его, постоянно снабжая вашу команду данными, необходимыми для обнаружения мошенничества в реальном времени, до совершения транзакции. Наше решение позволяет вашим системам использовать дополнительный контекст для более быстрого и точного принятия решений, а также для интеллектуального и адаптивного использования поэтапной аутентификации.

Свяжитесь с нами, чтобы узнать больше: kfp@kaspersky.com

www.kaspersky.ru