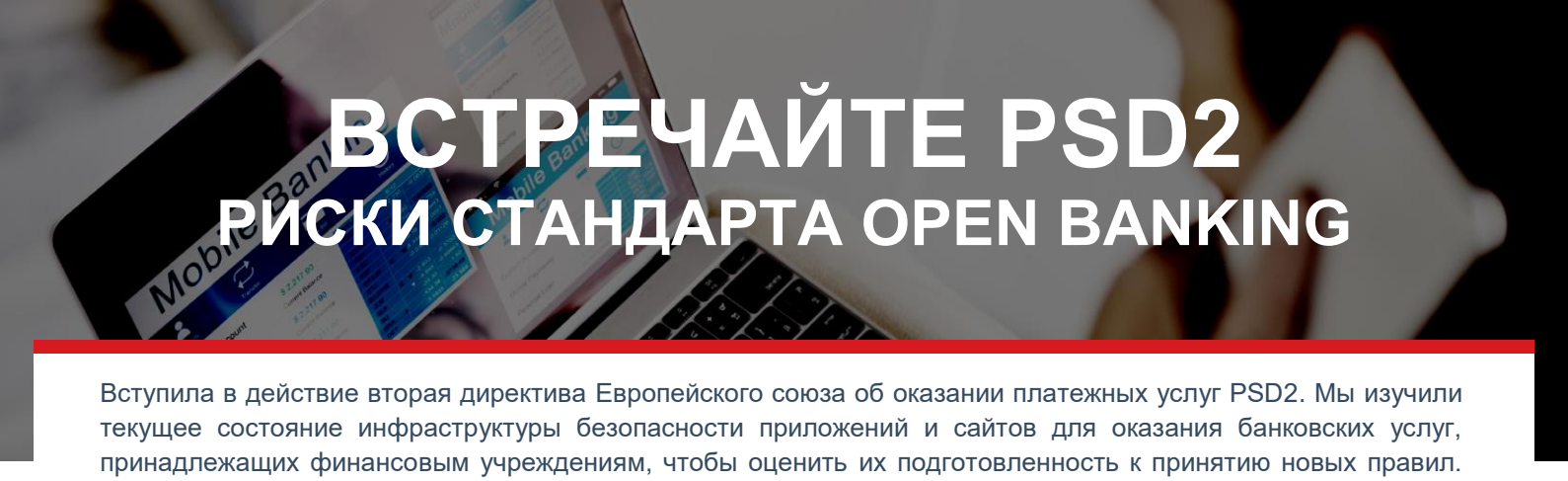

ВСТРЕЧАЙТЕ PSD2
РИСКИ СТАНДАРТА OPEN BANKING

Вступила в действие вторая директива Европейского союза об оказании платежных услуг PSD2. Мы изучили текущее состояние инфраструктуры безопасности приложений и сайтов для оказания банковских услуг, принадлежащих финансовым учреждениям, чтобы оценить их подготовленность к принятию новых правил. Директива, также известная как Open Banking, устанавливает меры безопасности в том числе и для финансово-технологических компаний, обрабатывающих данные клиентов.

Мы обнаружили, что такие приложения и сайты имеют уязвимости, требующие устранения, помимо внедрения новых мер безопасности в соответствии с директивой. Кроме того, новая директива расширяет поверхность кибератак, но от этого можно защититься, если подходить к решению проблемы в первую очередь с точки зрения безопасности.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

В исследовании мы подробно останавливаемся на основных результатах:

- Новые финансово-технологические компании имеют мало опыта противодействия мошенничеству, в отличие от известных банков. Несмотря на это, клиенты вынуждены будут оказывать им такое же доверие, которое банки завоевывали годами в качестве официальных сторонних поставщиков услуг.
- Пользователи приложений формата Open Banking более уязвимы перед фишинговыми атаками, т. к. хакеры используют приложения как приманку, чтобы получить конфиденциальную информацию.
- Мы обнаружили, что некоторые приложения для оказания банковских услуг используют прикладные программные интерфейсы API, раскрывающие персональные данные клиентов в URL-ссылках. Можно предположить, что злоумышленники будут искать и другие уязвимости для кражи данных и получения прибыли.
- Мобильные приложения для оказания банковских услуг связаны со сторонним ПО (например, для создания отчетов об ошибках и сбоях в работе), которое обменивается данными со сторонними веб-сайтами, что делает онлайновые банковские операции еще более уязвимыми.
- Финансово-технологические компании собирают данные с использованием небезопасных методов и устаревших систем (отслеживание движений курсора, ранние версии OFX и т. д.). Это должно быть запрещено в соответствии с директивой, но заинтересованные лица протестуют против запрета, ссылаясь на отсутствие известных атак или прецедентов.
- В финансовом секторе Соединенного Королевства планировалось внедрить FAPI (API финансового класса) помимо базовых требований директивы PSD2. Решение должно было дополнительно защитить данные, собираемые финансово-технологическими компаниями. Однако мы обнаружили, что оно еще не готово к использованию и может привести к появлению новых сценариев атак.

РЕКОМЕНДАЦИИ

- Банки и финансово-технологические компании должны придавать первостепенное значение безопасности и защите интересов клиентов.
- Финансово-технологические компании должны внедрять безопасные протоколы и процедуры.
- Банки и финансово-технологические компании не должны раскрывать персональные данные и другую критически важную информацию о сеансе связи в URL-ссылках. Даже зашифрованные данные могут быть украдены разными способами, что подвергает клиентов риску.
- Финансовый сектор на протяжении многих лет является одной из основных целей киберпреступников. Разработчики приложений формата Open Banking должны разрабатывать безопасное ПО и регулярно проводить аудит безопасности всех аспектов и компонентов своих проектов.
- Пользователи приложений формата Open Banking должны тщательно изучать приложения и поставщиков, прежде чем устанавливать приложения и доверять им доступ к своим банковским данным.

В исследовании «Встречайте PSD2: риски стандарта Open Banking» мы проанализировали безопасность финансового сектора в условиях смещающейся парадигмы вслед за принятием директивы PSD2.

TREND MICRO | research