УДК 343.7

Миронова Дарья Александровна,
студентка магистратуры
3 курс, специальность «Юриспруденция»
Средне-Волжский институт (филиал)
ВГУЮ (РПА Минюста России)
Россия, г. Саранск

РАЗНОВИДНОСТИ МОШЕННИЧЕСТВА В СТРАНАХ ЕВРОПЫ: КРАТКИЙ АНАЛИЗ

Аннотация: *статья посвящена видам мошенничества в странах Европы. Рассматриваются основные виды преступных действий, в том числе с использованием электронных средств платежа и выплат от государства.*

Ключевые слова: *мошенничество, преступление, Европа, контроль платежей.*

Annotation: *the article is devoted to the types of fraud in European countries. The main types of criminal acts are considered, including those involving the use of electronic means of payment and payments from the state.*

Key words: *fraud, crime, Europe, payment control.*

Существуют различные определения мошенничества с платежами, но, проще говоря, оно описывает незаконную транзакцию, которая отвлекает деньги или создает ложные/несанкционированные платежи от жертвы. Это часто достигается путем кражи их личной платежной информации или обманом, чтобы они поделились ею [1].

В отчете о мошенничестве и контроле платежей за 2022 год сообщается, что 71% организаций стали жертвами атак/попыток мошенничества с

платежами в 2021 году, которые обошлись предприятиям в миллиарды долларов по всему миру.

Клиенты должны быть уверены, что их деньги в надежных руках. Но одним из самых сложных аспектов выявления мошенничества с платежами и борьбы с ним является сложность взаимосвязанных сетей, лежащих в его основе.

Учитывая потенциальные атаки со всех сторон, крайне важно применять упреждающий и скоординированный подход к борьбе с мошенничеством с платежами и транзакциями, особенно в условиях повышенного риска киберпреступности. Кибербезопасность в настоящее время является главной проблемой отделов комплаенса в коммерческих организациях.

Существует множество видов мошенничества с платежами/транзакциями, в том числе:

Фишинг - электронные письма или веб-сайты, которые побуждают людей раскрывать личную информацию, такую как пароли и номера кредитных карт.

Кража личных данных

Вредоносное ПО — существует во многих формах, но количество программ-вымогателей, в частности, продолжает расти.

Мошенничество с платежными картами - без карты (обычно при покупках в Интернете) и с картой

Мошенничество, связанное с денежными мулами - часто невольные новобранцы используются для отмывания доходов от онлайн-мошенничества и мошенничества (обычно используется в APP - см. Ниже)

В Великобритании мошенничество с санкционированными push-платежами (APP) выросло на 71% в первой половине 2021 года, при этом сумма изъятий впервые превысила убытки от мошенничества с картами. При мошенничестве с приложениями клиента обманом заставляют авторизовать платеж на счет, контролируемый преступником, или передать личные данные

и пароли с помощью мошеннических телефонных звонков, текстовых сообщений и электронных писем, поддельных веб-сайтов и сообщений в социальных сетях.

Одним из самых прибыльных видов мошенничества с платежами является Advanced Persistent Threat (APT), в котором используются сложные методы взлома для получения несанкционированного доступа к компьютерным сетям с целью кражи данных.

APT часто спонсируются государством и, согласно Европейскому платежному совету (EPC), «должны рассматриваться как потенциальный высокий риск не только для платежных инфраструктур, но и для всех платежных экосистем, связанных с сетью».

(Распределенный) отказ в обслуживании (D)DoS) – Ддос -атака – это форма мошенничества с онлайн-платежами, при которой преступники стремятся сделать компьютеры или сети недоступными для пользователей, чтобы нарушить работу услуг, часто через ботнеты (захваченные компьютерные сети, контролируемые хакером). Количество (D)DoS-атак остается высоким, и EPC предупреждает о систематических нападениях на финансовый сектор.

Красные флажки платежного мошенничества

Серьезной проблемой в области мошенничества с платежами является понимание различий между хорошими и плохими транзакциями и принятие решения о том, как откалибровать автоматизированные решения для обнаружения мошенничества для сбора соответствующей информации.

В то время как некоторые отклонения от типичного профиля клиента должно быть легко обнаружить — адреса доставки слишком далеко от IP-адреса, несоответствие информации и т. д. — мошенники становятся все более изощренными и все более осторожными в устранении любых пробелов. Это означает, что фирмы должны проявлять бдительность и проявлять должную осмотрительность при проверке расхождений.

Риски мошенничества с платежами, которых следует опасаться, включают:

Фишинг – срочные или угрожающие формулировки, запросы конфиденциальной информации, несоответствие информации, подозрительные вложения, непрофессиональный дизайн, несовпадение URL/адресов электронной почты, отправитель не обращается к жертве по имени

Кража личных данных — необъяснимые списания или снятие средств, документы, предоставленные для удостоверения личности, выглядят измененными или поддельными, предоставлена подозрительная или противоречивая информация, превышение кредитных лимитов.

Вредоносное ПО — программное обеспечение внезапно требует обновления информации; оповещение предупреждает, что устройство заполнено вирусами, на экране внезапно появляются предложения о сканировании систем

Мошенничество с платежами по картам — крупные заказы или заказы на несколько количеств одного и того же товара, необычные трансграничные транзакции, выдача крупных сумм наличными или покупка предметов роскоши, всплески активности

APT — адресные фишинговые электронные письма, странные входы в систему, перемещенная информация, широко распространенный троян-бэкдор, данные собраны и готовы к экспорту.

(D) Dos-атаки – медленный доступ к файлам, чрезмерное количество спам-писем, проблемы с доступом к веб-сайтам, отключение интернета

Как снизить риски мошенничества с онлайн-платежами

Подход, основанный на оценке рисков, основанный на профилях клиентов, безопасности и потоках платежей, является ключом к надежной программе снижения рисков мошенничества с платежами, наряду с осведомленностью сотрудников и клиентов о тревожных сигналах.

Список источников:

1. Что такое мошенничество в платежах? // What is Payment Fraud? | ComplyAdvantage (дата обращения: 10.10.2022).