Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Воздействие компьютерных атак на финансовые организации Российской Федерации

Научный руководитель – Нургазина Гульмира Есимбаевна

Целищева Дарья Дмитриевна

Студент (бакалавр)

Российская государственная академия интеллектуальной собственности, Москва, Россия

E-mail: Dasha.ts15@mail.ru

Ежегодно российские банки сталкиваются с всевозможными разновидностями атак на свои информационные системы (ИС). Данные атаки целенаправленны- начиная от кражи персональных данных клиентов и сотрудников финансовых организаций и заканчивая заражением программного обеспечения (ПО) банка. [1]

В настоящее время эти атаки направлены на:

1. Процессинг банковских карт. Злоумышленники стараются пробраться в информационные системы банка с помощью ботов и заражения сети для увеличения баланса краденых карт с дальнейшим снятием валюты за рубежом. [2]
2. Систему SWIFT. Глобальная система оповещений SWIFT считается лакомым кусочком для злоумышленников. К примеру, с помощью вирусного ПО Trojan PDF reader, кибер-преступники в феврале 2016 смогли ограбить Центральный банк Бангладеша на сумму 81 млн. долларов. [3]
3. Банкоматы. Так, в августе 2019 года банкоматы компании NCR с валидаторами HBV, ABV, RBV стали принимать игрушечные деньги из-за устаревшего ПО. [4]

Перечисленные выше атаки на финансовые организации РФ СМИ старается не публиковать в связи с репутационными рисками бизнеса. Чаще всего они отсылают сведения о кибер-атаках в структурное подразделение Департамента информационной безопасности Банка России - ФинЦЕРТ. Полученная информация в основном публикуется в обзорах без уточнения названия организаций.

Что же является причинами, побудившими кибер-преступников атаковать банки РФ? Ими могут быть:

- отсутствие своевременного обновления безопасности популярного офисного ПО, в том числе Microsoft Office, операционных систем;
- отсутствие актуального обновления антивирусного программного обеспечения на рабочих столах сотрудников банка;
- отсутствие контролируемого доступа сотрудников к важным для организации информационным системам (таким, как системы переводов денежных средств, процессинг банковских карт и пр.);
- массовое использование учетных записей с преимуществами локальных администраторов, безосновательная дача преимуществ сотрудникам в разных информационных системах;
- использование легких паролей;
- наличие неконтролируемого доступа в глобальную сеть Интернет.

Злоумышленники легко приспосабливаются к регулярно изменяющимся обстоятельствам, постоянно мониторят новости на форумах, где обсуждаются схемы эксплуатации новейших и популярных уязвимостей программного обеспечения. В этих форумах можно

найти большое количество подробного описания вариантов атак на банки, в том числе как незаконно вывести средства за границу. Также здесь можно найти предложения услуг от криминальных структур, обладающих связями в финансовых организациях, по выпуску поддельных банковских карт для снятия средств с «атакованных» банкоматов страны.

Существует несколько этапов атак на финансовые организации РФ [5]:

1. Предварительная разведка и подготовительные работы.
2. Проникновение во внутреннюю сеть банка.
3. Закрепление во внутренней сети и развитие атаки.
4. Компрометация банковских систем и хищение средств.
5. Устранение следов преступления.

Таким образом, в настоящее время финансовая безопасность банковского сектора РФ является актуальной проблемой и требует снижения внешних атак и обеспечения безопасности информационных систем банков.

Источники и литература

1) 1. Аналитики Solar JSOC предупреждают о росте количества сложных атак на банки. -URL: https://ib-bank.ru/bisjournal/news/11538 (дата обращения: 03.03.2021).
2) 2. ЦБ: Киберпреступники переключились с карточек на банковский процессинг. - URL: https://www.finanz.ru/novosti/lichnyye-finansy/cb-kiberprestupniki-pereklyuchilis-s-kartochek-na-bankovskiy-processing-1002213538 (дата обращения: 03.03.2021).
3) 3. SWIFT оповестил, что второй банк пострадал от атаки вредоносных программ. -URL: https://www.reuters.com/article/swift-heist-idUSL2N18A00R (дата обращения: 03.03.2021).
4) 4. Тысячи банкоматов в России принимают игрушечные деньги из-за устаревшего ПО. - URL: https://news.myseldon.com/ru/news/index/215441914 (дата обращения: 03.03.2021).
5) 5. Атаки на банки. - URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Banks-attacks-2018-rus.pdf (дата обращения: 03.03.2021).