УДК 336.717

ВЛИЯНИЕ КИБЕРАТАК НА КРЕДИТНО-ФИНАНСОВЫЕ ОРГАНИЗАЦИИ РФ ЗА ПЕРИОД 2018-2022 ГГ

Танич К.Д.
студент, кафедра прикладной математики и компьютерной безопасности, Институт космических и информационных технологий СФУ, РФ, г. Красноярск

Федоров Г.А.
студент, кафедра прикладной математики и компьютерной безопасности, Институт космических и информационных технологий СФУ, РФ, г. Красноярск

Зябликов Д.В.
научный руководитель, кандидат экономических наук, доцент кафедры «Экономики и управления бизнес-процессами», Институт управления бизнес-процессами СФУ, РФ, г. Красноярск

Аннотация
В данной статьей описывается, как кибератаки влияют на финансовый сектор, в период 2018-2022 гг, какие тактики чаще всего используют атакующие для достижения своих целей, а также объем потерь кредитно-финансовых организаций и их клиентов из-за хакерских атак и какие меры принимает ФинЦЕРТ[1] в связи с деструктивными действиями со стороны злоумышленников.

Ключевые слова: кибератаки, кредитно-финансовые организации, экономический ущерб кредитно-финансовых организаций, финансовый сектор.

IMPACT OF CYBER-ATTACKS ON RUSSIAN FINANCIAL INSTITUTIONS IN 2018-2022

Tanich K.D.
Student, Department of Applied Mathematics and Computer Security, Institute of Space and Information Technologies, SFU, Russian Federation, Krasnoyarsk

[1]Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, специальное структурное подразделение Банка России

Fedorov G.A.
Student, Department of Applied Mathematics and Computer Security, Institute of Space and Information Technologies, SFU,
Institute of Space and Information Technologies, Siberian Federal University, Russia, Krasnoyarsk

Zyablikov D.V.
supervisor,
D. in Economics, Assistant Professor of Economics and Business Process Management Department, Institute of Business Process Management, SFU, Russian Federation, Krasnoyarsk

Abstract
This article describes how cyberattacks affect the financial sector, in the period 2018-2022, what tactics attackers most often use to achieve their goals, as well as the volume of losses of credit and financial institutions and their customers due to hacking attacks and what measures FinCERT takes in connection with destructive actions by attackers.

Keywords:cyber attacks, financial institutions, economic damage to financial institutions, financial sector.

Введение

В наше время люди всё чаще и чаще используют разные электронные устройства с доступом в интернет для хранения своих персональных данных, банки используют приложения для действия с деньгами, компании переводят свои процессы на автоматизированные линии. В связи с этим появляется много вопросов, один из них – как сохранить все эти данные в безопасности, не подвергнуть их различным угрозам.

Сфера информационной безопасности с недавних пор является неотъемлемой частью бюджета многих компаний. Многие компании с каждым годом подвергаются кибератакам с увеличивающейся частотой, поэтому приходится увеличивать бюджеты организаций, наращивать производственную мощь. Однако не всегда это выгодно, потому что защита может оказаться дороже, чем потенциальные последствия после некоторых атак.

Как атакуют злоумышленники

Информационная безопасность – один из главных приоритетов финансового сектора. На данный момент, большинство финансовых организаций имеют сложную информационную систему (ИС), которая может включать в себя: голосовые помощники, чат-боты, веб-приложения, мобильные приложения. Также нужно предусматривать возможности для масштабирования ИС, так как количество пользователей постоянно растет. В связи с этим, поверхность для атаки со стороны злоумышленников увеличивается, что в свою очередь заставляет государство реагировать на эти инциденты принимать меры для большего контроля и для обеспечения безопасности клиентов.

Защищенность организаций кредитно-финансовой сферы растет быстрыми темпами, однако же защищенность некредитных финансовых организаций не развивается так стремительно, поэтому государству пришлось вносить поправки в законы. В связи с этим произошли изменения в ФЗ-№167, принятыми Советом Федерации20 июня 2018 года, число подконтрольных ЦБ РФ организаций в сфере кредитно-финансовой сфере стало увеличиваться. [10] На конец 2017 года в информационном обмене участвовало лишь 418 компаний и филиалов, на конец 2018 года таких компаний стало уже 718, причем более половины из них составляли банковские организации. Также организации обязали сообщать о всех инцидентах информационной безопасности, в частности о переводах без согласия клиентов. [5]

За 2019-2020 гг ЦБ РФ описал следующие виды атак.

- Атаки на информационные ресурсы компаний РФ в кредитно-финансовой сфере. Активность злоумышленников в этом направлении понемногу уменьшается, в первую очередь это связано с улучшением защищенности информационных инфраструктур организаций.
- Атаки на информационные ресурсы клиентов кредитно-финансовой сферы Российской Федерации. За 2019-2020 годы центр

мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) получил информацию о 225 атаках данной группы.Из этих данных можно сделать вывод, что в среднем атаки происходили 2-3 раза в неделю, что указывало на интенсивную работу групп Remote Transaction Manager (RTM), другие виды вредоносного программного обеспечения (ВПО) были замечены в единичных случаях.

- Атаки с использованием программ-шифровальщиков. ФинЦЕРТ было замечено большое количество запросов участников информационного обмена по фактам распространения различных программ-шифровальщиков. Основным способом распространения данных программ является рассылка по электронной почте сообщений, содержащих ссылки на вредоносные файлы.
- Атаки «отказ в обслуживании». ФинЦЕРТ получил 221 сообщений от участников информационного обмена об инцидентах, связанных с атаками типа «отказ в обслуживании» (DoS). Был выявлен рост атак типа SYN-Flood. В 2020 году были замечены особые случаи, например, были отмечены DoS атаки направленные на нарушение работы веб-приложений на прикладном уровне сетевой модели Open Systems Interconnection(OSI)
- Атаки на банкоматы. В 60% случаев злоумышленники используют физическое воздействие на банкоматы. В 2019 году была зафиксирована атака через уязвимость EternalBlue, которая позволяет выполнять произвольный код с высокими привилегиями, но она была заблокирована. Также в конце 2020 года были зафиксированы атаки с использованием ПО Cutlet Maker. Одна из них привела к хищению порядка 1,5 млн рублей.
- Атаки с использованием социальной инженерии. Исходя из данных, полученных ФинЦЕРТ по каналам информационного обмена, на финансовом рынке наблюдается увеличение количества атак на клиентов

кредитных организаций. Количество инцидентов выросло на 88% по сравнению с 2019 годом. Основным видом атаки является фишинг.

Стоит отметить, что пандемия COVID-19 внесла свои коррективы, и большинству кредитно-финансовым организациям пришлось перестроиться на удаленную работу, что в свою очередь способствовало росту количества мошеннических сайтов в кредитно-финансовой сфере.

В период пандемии COVID-19 (2020-2021 гг) ФинЦЕРТ зафиксировал значительный рост количества фишинговых рассылок, а также мобильного мошенничества, совершаемого в отношении граждан. В этот период в большей степени использовались темы рассылок: компенсации, государственные пособия и государственная поддержка. Фишинговые сайты социальных служб встречались в 43% случаев. За период пандемии, благодаря взаимодействию с регистраторами доменных имен, перестали быть доступны 4314 сайтов мошеннического характера из 5011 направленных.

Как следует из отчета ЦБ, в третьем квартале 2021 года значительно возросли фишинговые атаки, направленные на клиентов финансовых организаций, 1995 в сравнении с 273 за тот же период 2020 года. Количество атак, направленных на клиентов финансовых организаций и атак с использованием методов социальной инженерии, также возросло по сравнению с прошлым годом соответственно 12211 и 4634. Количество атак с помощью ВПО осталось примерно на том же уровне 93 и 107. Уменьшилось количество атак направленных на эксплуатацию уязвимостей ПО 42 и 22.[3] Данных об инсайдерских утечках ЦБ не предоставляет.

Как считает RTM group - ведущая консалтинговая компания в области информационной безопасности, судебной экспертизы и ИТ-права, число внутренних утечек возрастет с 30% в 2021 до 50% в 2022 году. При этом доля хищений в категории внешних атак снизится с 15% до 3%.

Потери организаций от киберпреступности

Закономерно росту числа кибератак возрастает и ущерб на экономику организаций. В свою очередь, восстановление инфраструктуры стоит денег, а также компании теряют прибыль, которую могли бы получить при безостановочной работе. Исходя из исследований, можно представить, что 1 день остановки работы в крупном банке или финансовой организации может принести ущерб на несколько десятков миллионов.

Сами кредитные организации, а не их клиенты, становятся очень редкими пострадавшими в кибератаках, однако такие случаи происходят. Согласно пресс-релизу Group-IB в феврале 2021 года, один из банков РФ подвергся атаке, в ходе которой потерял 500 млн. рублей со своего корреспондентского счета. В ходе расследования было обнаружено, что атака на банк была тщательно спланирована, она началась еще летом 2020 года с дочернего предприятия, после чего мошенники проникли в сеть банка и полгода анализировали ее.[1] Этот случай демонстрирует, что атаки на сами банки приносят множество затрат по времени, однако, из-за огромного количества денежных средств, которые можно украсть, они являются прибыльными.

Кроме крупных атак, иногда появляется информация о малых кражах. В 2020 году, в Свердловской области были задержаны трое подозреваемых. Мошенническая схема заключалась в следующем. На заправке опускался пистолет в бак авто или же канистру, после чего на онлайн терминале вводились данные карты, после начала заправки карту меняли на другую, где отсутствовали средства. Так как средств на карте не было, банку приходилось оплачивать заправку за свой счет. С помощью этой схемы, злоумышленники похитили более 1 мил. рублей. [8] Эта ситуация дает нам понять, что кредитно-финансовый сектор, может быть не защищен от атак простых людей, которые не относятся к хакерским группировкам.

Основополагающие потери экономики в кредитно-финансовой сфере, это сами клиенты организаций, а точнее их действия по отношению к деньгам. В

Российской Федерации, по данным ФинЦЕРТ, объем несанкционированных операций со счетов клиентов организаций кредитно-финансового по итогам 2018 г. составил 2,885 млрд руб. На 2019 год объем данных операций составил 6,424 млрд рублей. Из отчета ЦБ РФ за 2021 году количество и объем операций без согласия клиентов составили соответственно 1 035 тыс. единиц и 13 582 млн. рублей по сравнению с 2020 годом увеличение составило 33,8% и 38,8%. [2] Основываясь, на этих данных можно заявить, что, если организации не начнут уделять должного внимания безопасности, то эта цифра будет расти с каждым годом.

Однако официальная статистика ЦБ РФ отличается от сумм, которые представил Генпрокурор в годовом отчете за 2019 год, согласно документу, со счетов россиян было похищено более 232 млрд руб, в 2018 году более 171 млрд. Также стоит отметить, что уровень возврата средств падает второй год подряд на фоне роста хищений. Согласно статистике ФинЦЕРТа на 2019 год процент возврата составил лишь 9,3% украденных средств, 2020 вернулось лишь 8,7, а в 2021 эта цифра снизилась до 6,8%.

Вывод

Таким образом, можно сделать вывод, что влияние кибератак на кредитно-финансовые организации очень разнообразное. Первое - конечно же ущерб, который несут организации и их клиенты в том числе. Исходя из статистики видно, что меры всегда принимаются уже после инцидентов, поэтому защитные меры всегда следуют за кибератаками. Второе - меры принимаемые ЦБ РФ и в частности ФинЦЕРТом, демонстрируют положительный эффект, видно как некоторые атаки теряют свою актуальность и злоумышленники все чаще пытаются пробраться в инфраструктуру организации с помощью методов социальной инженерии, все больше организаций становится подконтрольными ЦБ РФ, вследствие чего

отслеживать новые атаки и организовывать совместную защиту становится проще.

Также кредитно-финансовые организации продемонстрировали гибкость и в условиях пандемии в кратчайшие сроки смогли адаптироваться к удаленной работе и обеспечить высокий уровень защиты своей инфраструктуры.

Библиографический список:

1. Group-IB сообщила о хищении хакерами средств с корсчета банка в ЦБ. [Электронный ресурс]. — Режим доступа — URL: https://www.kommersant.ru/doc/5130099(Дата обращения 27.04.2022)

2. Обзор операций, совершенных без согласия клиентов финансовых организаций в 2021 году. [Электронный ресурс]. — Режим доступа — URL:https://www.cbr.ru/analytics/ib/operations_survey_2021/(Дата обращения 28.04.2022)

3. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. — Режим доступа — URL: https://www.cbr.ru/analytics/ib/review_3q_2021/(Дата обращения 28.04.2022)

4. Основные типы компьютерных атак в кредитно-финансовой сфере в 2019-2020 годах. [Электронный ресурс]. — Режим доступа — URL: https://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf(Дата обращения 22.04.2022)

5. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере департамента информационной безопасности банка России 1.09.2017 - 31.08.2018. [Электронный ресурс]. — Режим доступа — URL:https://www.cbr.ru/Collection/Collection/File/32088/survey_0917_0818.pdf(Дата обращения 22.04.2022)

6. Потери организаций от киберпреступности. [Электронный ресурс]. — Режим доступа — URL: https://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности(Дата обращения 28.04.2022)

7. Сага об инсайдах. [Электронный ресурс]. — Режим доступа — URL: https://www.kommersant.ru/doc/5216772(Дата обращения 28.04.2022)

8. Свердловские мошенники похитили у банка 1 млн руб. с помощью уникальной схемы [Электронный ресурс]. — Режим доступа — URL: https://www.securitylab.ru/news/513428.php(Дата обращения 28.04.2022)

9. Сколько стоит безопасность. Анализ процессов обеспечения иб в российских компаниях. [Электронный ресурс]. — Режим доступа — URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf(Дата обращения 22.04.2022)

10. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств" от 27.06.2018 N167-ФЗ.[Электронный ресурс]. — Режим доступа — URL:http://www.consultant.ru/document/cons_doc_LAW_301060/(Дата обращения 22.04.2022)

Оригинальность 85%