О ТЕНДЕНЦИЯХ ИЗМЕНЕНИЯ КИБЕРУГРОЗ В ФИНАНСОВО-КРЕДИТНОЙ СФЕРЕ ПО ДАННЫМ БАНКА РОССИИ

ON TENDENCIES OF CHANGING CYBER THREATS IN FINANCIAL AND CREDIT SPHERE ACCORDING TO THE DATA OF BANK OF RUSSIA

V. Nikolaev
T. Kulakova

Summary. Object. The article discusses changes in the methods of computer attacks based on the results of information security incidents in the financial sector.

Methods. For the analysis, the reports of the Financial Sector Computer Emergency Response Team (FinCERT Bank of Russia) were used.

Findings. The growth of hardware and software security of Russian information systems is confirmed, and, in this connection, the shift of the center of gravity of computer attacks to the field of social engineering.

Conclusisons. The lack of qualification of personnel and users of information systems in the sphere of information security is becoming the main threat to the digital economy.

Keywords: security, cyber threat, monitoring, phishing, mining, spam.

Николаев Владимир Вениаминович
К.т.н., доцент, Среднерусский институт управления — филиал РАНХиГС
nikolaev.vlad@gmail.com
Кулакова Татьяна Александровна
Преподаватель, Банковский колледж Среднерусского института управления — филиала РАНХиГС
kulakova057@gmail.com

Аннотация. Цель: В статье рассматриваются изменения в методах компьютерных атак по результатам инцидентов информационной безопасности в финансовой сфере.

Методы. Для анализа использованы отчеты Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России).

Результаты. Подтверждается рост аппаратно-программной защищенности российских информационных систем и, в связи с этим, перенос центра тяжести компьютерных атак в область социальной инженерии.

Выводы. Недостаточный уровень квалификации персонала и пользователей информационных систем в сфере информационной безопасности становится основной угрозой для цифровой экономики.

Ключевые слова: безопасность, киберугроза, мониторинг, фишинг, майнинг, спам.

Введение

1 мая 2019 года Президент Российской Федерации подписал Федеральный закон № 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [1]. По замыслу авторов законопроекта, его главной целью является сохранение работоспособности российского сегмента Интернета при его отключении от глобальной сети, а также упрощение процедуры блокировки сайтов с законодательно запрещенным контентом. Для этого предполагается изменение маршрутизации данных пользователей через специальные точки приема-передачи информации и планы по созданию российской системы доменных имен. Если смотреть с технической точки зрения, то подобная система, известная как "Золотой щит" (или, неофициально, "Великий китайский файрвол") уже создана в Китайской народной республике. Её стоимость по оценкам экспертов составила приблизительно 800 миллионов долларов и её постоянную работу обеспечивают 30 тысяч сотрудников. Опасения российских пользователей связаны с тем, что реализация этого закона в Российской Федерации приведет к тому, что, очевидно, практически все рычаги управления Рунетом будут сосредоточены в руках одной организации — Роскомнадзора.

Говоря о национальной системе доменных имен, необходимо помнить, что работу глобальной сети Интернет обеспечивают 13 корневых серверов службы доменных имен DNS, управляемых двенадцатью различными организациями, независимыми от ICANN (Internet Corporation for Assigned Names and Numbers), изначально занимавшейся администрированием доменных имен и IP-адресами в глобальной сети. Общее число серверов DNS значительно больше — например, в России по состоянию на 2018 год уже было размещено 11 реплик корневых серверов DNS пяти имен. При этом надо иметь в виду, что только до трети запросов пользователей требуют обращения к одному из корневых серверов.

По данным за 2019 год российская доменная зона. RU по числу доменов — более 5 миллионов — занимает пятое место в Интернете среди национальных доменов. Права администрирования национальных доменов верхнего уровня в России принадлежат автономной некоммерческой организации "Координационный центр доменов.RU/.РФ". Прекращение делегирования домена (временная блокировка доменного имени до устранения причины) или аннулирование регистрации домена может выполняться на основании судебного акта или решения компетентной организации, в частности, ФСБ, МВД, Роскомнадзора, Центрального Банка РФ, Лаборатории Касперского.

Технические и организационные вопросы блокировки запрещенного контента являются актуальными в том числе и при отражении кибератак на организации финансово-кредитной сферы.

Материалы и методы

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ В. В. Путина 5.12.2016 года, констатируется, что состояние информационной безопасности характеризуется "постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты информационной инфраструктуры" [3].

Рассмотрим тенденции изменения угроз кибербезопасности в такой чувствительной сфере, касающейся как отдельного человека, так и государства в целом, как финансовая.

В соответствии с поручением Совета Безопасности Российской Федерации в структуре Главного управления безопасности и защиты информации (ГУБиЗИ) Банка России в июне 2015 года создан Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — ФинЦЕРТ (FinCERT). Деятельность Центра базируется на соблюдении законодательства РФ в области защиты банковской тайны и обеспечении конфиденциальности, целостности и доступности хранимой и передаваемой информации [2]. Основными задачами ФинЦЕРТ являются организация обмена информацией и анализ инцидентов информационной безопасности, а также формирование аналитических материалов и подготовка рекомендаций в области обеспечения защиты информации в финансовой сфере.

Любое юридическое лицо, осуществляющее лицензированную финансовую деятельность, может стать участником информационного обмена. В обмене информацией также участвуют разработчики банковского программного обеспечения и антивирусных программ, операторы связи, правоохранительные органы и федеральные и региональные органы государственной власти. Участие в информационном обмене изначально являлось добровольным, но с 1.07.2018 года кредитные организации должны уведомлять Банк России об инцидентах информационной безопасности. Для повышения оперативности обмена информацией создана автоматизированная система обработки инцидентов (АСОИ ФинЦЕРТ), к которой подключены все банки Российской Федерации.

Литературный обзор

Сотрудничество с ФинЦЕРТ дает возможность финансовым (и не только) организациям оперативно узнавать об основных типах и механизмах реализации кибератак, а также об успешных методах противодействия подобного рода атакам.

Ранее многие банки не сообщали в Банк России об успешных хакерских атаках, если речь не шла о значительных суммах. Главная причина этого — репутационные риски, поскольку в случае утечки информации возможен отток клиентов. В 2016 году Банк России разработал обязательное для всех участников платежной системы Банка России положение, согласно которому вводится обязанность в течение трех часов информировать ФинЦЕРТ о выявленных или возможных инцидентах, связанных с нарушениями требований к обеспечению защиты информации в платежной системе.

Результаты деятельности ФинЦЕРТ с 1 июня 2015 г. по 31 августа 2018 года обобщены в годовых отчетах. Среди основных показателей деятельности ФинЦЕРТ отмечено, что число организаций — участников информационного обмена достигло 718, причем рост их числа на последний год составил 16%.

Отчеты ФинЦЕРТ за последние три года [7–9] позволяют выявить следующие остающиеся неизменными недостатки в области информационной безопасности у организаций кредитно-финансовой сферы, которые привели к удачным кибератакам:

- недостаточная грамотность персонала в области информационной безопасности, в частности, при открытии электронных писем, пришедших извне;
- отсутствие средств антивирусной защиты либо устаревшие вирусные базы;
- отсутствие сегментирования локальных вычислительных сетей для обеспечения независимого выполнения технологических процессов банковских операций.

Вновь проявившиеся недостатки могут быть объяснены недостаточным пониманием сотрудниками серьёзности требований к работе персонала в информационных системах и недостаточной квалификацией специалистов по информационным системам:

- использование слабых паролей либо хранение паролей в открытом виде;
- отсутствие установленных актуальных обновлений операционной системы MS Windows и офисного пакета MS Office, что позволяет злоумышленникам использовать известные уязвимости программного обеспечения;
- неправильная настройка межсетевых экранов;
- отсутствие или неправильная настройка средств обнаружения и предотвращения вторжений, позволяющее нарушителю длительное время скрытно находиться в сети.

Надо заметить, что в то же время появление этих новых причин говорит также о серьезном совершенствовании технического обеспечения информационных систем организаций кредитно-финансовой сферы за последние годы.

В качестве причин успешности целевых атак потеряли свою актуальность ненадлежащий контроль руководством кредитной организации установленной технологии работы с данными, присвоение пользователям избыточных прав локального администратора и отсутствие блокировки автоматического запуска макросов в документах Microsoft Office.

Таким образом, можно отметить, что, наряду с отдельными случаями несоблюдения элементарных принципов работы в компьютерных сетях, большая часть уязвимостей в настоящее время находится в области организационного обеспечения требований по поддержанию требуемого уровня информационной безопасности программного и аппаратного обеспечения.

Основными типами атак за отчетный период, зафиксированные ФинЦЕРТ, были:

- целевые атаки группировок злоумышленников на финансовые организации;
- спам-атаки на организации кредитно-финансовой сферы;
- атаки на клиентов кредитно-финансовых организаций с использованием методов социальной инженерии;
- атаки на клиентов банков с использование вредоносного программного обеспечения;
- атаки на устройства самообслуживания.

По данным ФинЦЕРТ за последнее время наблюдается, с одной стороны, рост числа целевых атак на банковскую инфраструктуру, с другой — значительное снижение ущерба от успешных атак: с 1,1 млрд. рублей за восемь месяцев 2017 года до 80 миллионов рублей за аналогичный период 2018 года.

Нецелевые спам-атаки отличаются чрезвычайно низкой эффективностью в связи с возможностью фильтрации электронных писем. В связи с массовостью рассылки по тысячам адресов какая-то крайне небольшая часть пользователей, получивших подобные письма, всё-таки попадается на удочку методов социальной инженерии. Этому может способствовать недостаточная компьютерная грамотность пользователей. По данным ФинЦЕРТ 75% спам-рассылки содержит различные майнеры — программы для добычи криптовалют. Особого вреда это вредоносное программное обеспечение (ПО) не наносит, если не считать значительной траты вычислительных ресурсов компьютера. Остальные 25% спама — это фишинговые письма, "выигрыши", реклама и письма с угрозами.

В настоящее время в связи с ростом защищенности кредитно-финансовых организаций происходит смещение вектора интереса злоумышленников в сторону клиентов кредитных организаций. Целью таких атак является установка вредоносного ПО и получение доступа к удаленному компьютеру, кража учетных данных пользователя к системам дистанционного банковского обслуживания, перехват реквизитов в платежных документах с целью создания подложных платежных поручений. Распространение вредоносного ПО происходит в основном через рассылки фишинговых писем с названиями, характерными для бухгалтерской или законодательной деятельности.

С января 2017 года ФинЦЕРТ стал принимать участие в блокировке фишинговых сайтов. С сентября 2017 года по август 2018 года по инициативе ФинЦЕРТ снято с делегирования 1668 доменов, использованных для мошенничества, в качестве лжебанков, микрофинансовых организаций, страховых компаний, электронных магазинов и т.д.

Иной вид, но с той же целью внедрения вредоносного ПО, имеют атаки, получившие название watering hole ("водопой"). Злоумышленники анализируют частоту посещения сотрудниками организации или обычными пользователями Интернет-ресурсов и взламывают сайты, пользующиеся популярностью, внедряя вредоносный скрипт. Этот скрипт может устанавливать вредоносное ПО на компьютер посетителя сайта.

Для атаки на физические лица — владельцев смартфонов используются телефонные звонки, рассылка СМС, вредоносное ПО, создающее окна приложений он-

лайн-банкинга. Широко используется взлом аккаунтов в социальных сетях с рассылкой просьб о материальной помощи. Уязвимостью является человеческий фактор — доверчивость и беспечность, используемые для доступа к платежным реквизитам граждан.

Основные виды атак на банковские терминалы или устройства самообслуживания остаются неизменными — это физический взлом устройства и проникновение на банкомат из внутренней сети банка с целью установки вредоносного ПО, обеспечивающего выдачу наличных денежных средств. Отмечено постоянное снижение атак типа скимминг и шимминг, предназначенных для копирования данных с магнитной ленты платежной карты, связанное с выпуском чипованных карт. Возросло число попыток мошенничества с отменой транзакций (TRF — Transaction Reversal Fraud) — воздействия на процесс обработки операции выдачи наличных средств. Целью атаки является принятие банкоматом ошибочного решения о необходимости обратного зачисления денежных средств. Один вариант атаки предполагает физическое повреждение шторки механизма с уже выданной денежной суммой, при этом банкомат прекращает обслуживание клиента, но восстанавливает баланс на счете карты. Второй вариант взлома использовал некорректные настройки некоторых процессинговых систем при переводе денежных средств от одного клиента к другому, позволяющие одновременно и выполнить зачисление на карту получателя и восстановить баланс на карте отправителя.

8 ноября 2016 года онлайн — ресурсы Сбербанка подверглись мощным DDoS — атакам. DDoS (Distributed Denial of Service) означает распределенную атаку типа "отказ в обслуживании". Атаки были организованы с ботнетов, включающих десятки тысяч компьютеров, территориально распределенных по разным странам. Ботнет — это сеть компьютеров, скрытно зараженных вредоносными программами и находящаяся под контролем злоумышленников. Система защиты Сбербанка вовремя обнаружила и локализовала кибератаку, сбоев в работе сервиса не было. В период чемпионата мира по футболу в 2018 году зафиксировано три DDoS-атаки, но применение предложенных ФинЦЕРТ превентивных мер показало свою эффективность, сведя потери к нулю.

В апреле 2017 года ФинЦЕРТ разослал участникам информационного обмена информацию о методах выявления рассылаемого по почте вредоносного ПО WannaCry типа "шифровальщик" и рекомендации по установке пакета обновлений безопасности для операционных систем Microsoft Windows. 12 мая была зафиксирована кибератака с использованием данного типа вредоносного ПО. По итогам атаки были зафиксированы лишь единичные инциденты, связанные с компрометацией ресурсов кредитных организаций, последствия которых были устранены в кратчайшие сроки. При атаках вирусов-шифровальщиков exPetr и BadRabbit в июне и октябре 2017 года банковский сектор практически не пострадал.

Результаты

Анализ инцидентов информационной безопасности, приведенный в отчетах ФинЦЕРТ, полностью согласуется с опытом разработки информационных систем [4, 5], подтверждая тот факт, что наибольшими возможностями для нанесения ущерба организации обладает её собственный персонал [6]. Всё большую угрозу представляет вектор методов социальной инженерии, связанный с недостаточной внимательностью или образованностью пользователей в области соблюдения требований информационной безопасности.

Обсуждение

Обмен информацией о зафиксированных кибератаках и наблюдаемых тенденциях развития векторов кибератак на информационные системы предполагает организацию оповещения ответственных сотрудников о зафиксированных инцидентах информационной безопасности, индикаторах компрометации систем, а также осуществляемых спам-рассылках и попытках внедрения вредоносного ПО. Организационные и технические решения, предлагаемые законом о защите Рунета, повысят эффективность процедуры разделегирования и аннулирования доменов, используемых для организации атак на российские информационные системы. Вместе с тем требуется существенное повышение уровня знаний в области информационной безопасности всех участников финансовых рынков в связи с использованием злоумышленниками человеческого фактора.

Заключение

Широкое использование методов социальной инженерии при организации кибератак на организации кредитно-финансовой сферы требует:

- повышения финансовой и информационной грамотности населения;
- разъяснительной работы со специалистами служб информационной безопасности;
- информирования населения о действиях банков для минимизации последствий инцидентов.

Информационный обмен позволяет организовать обмен опытом в борьбе с современными киберугрозами, повысить уровень компетенции, а так же выработку универсальных сценариев ликвидации последствий инцидентов информационной безопасности.

Благодарности

Автор выражает благодарность сотрудникам Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Центрального банка Российской Федерации на публикацию ежегодных отчетов, использованных для анализа тенденций изменения угроз в сфере информационной безопасности.

ЛИТЕРАТУРА

1. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1. (Дата обращения: 27.06.2019).
2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) "Об информации, информационных технологиях и о защите информации"// СПС КонсультантПлюс. [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_61798/. (Дата обращения: 27.06.2019).
3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646) // СПС КонсультантПлюс. [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_208191/. (Дата обращения: 27.06.2019).
4. Николаев В. В. Информационная система мониторинга фактического уровня защищенности образовательных учреждений // Информационное развитие России: состояние, тенденции и перспективы. Сб. науч. статей всерос. науч.-практ. конф. / Орел: Изд-во Среднерусского института управления — филиала РАНХиГС, 2017. — С. 120–126
5. Николаев В. В. Аспекты информационной безопасности при программировании на языке Java // Наука вчера, сегодня, завтра / Сб. ст. по материалам XLVIII междунар. науч.-практ. конф. № 7(41). — Новосибирск: Изд. АНС «СибАК», 2017. — С. 11–15
6. Стандарт Банка России СТО БР ИББС-1.0–2014 "Обеспечение информационной безопасности организаций банковской системы Российской Федерации". [Электронный ресурс]. — URL: http://www.cbr.ru/Content/Document/File/46921/st-10–14.pdf. (Дата обращения: 27.06.2019).
7. Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г. [Электронный ресурс]. — URL: http://www.cbr.ru/StaticHtml/File/14435/FinCERT_survey.pdf. (Дата обращения: 27.06.2019).
8. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России • 1 июня 2016–1 сентября 2017. [Электронный ресурс]. — URL: http://www.cbr.ru/StaticHtml/File/14435/GUBZI-4.pdf. (Дата обращения: 27.06.2019).
9. Отчет центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России • 1 сентября 2017–31 августа 2018. [Электронный ресурс]. — URL: http://www.cbr.ru/Content/Document/File/50959/survey_0917_0818.pdf. (Дата обращения: 27.06.2019).

Журнал «Современная наука: актуальные проблемы теории и практики»