УДК 004.056.5

В.А. Зайцев,
студент экономического факультета
Хабаровской государственной академии экономики и права
Н.А. Пономарёва,
канд. экон. наук, доцент,
профессор кафедры банковского дела
Хабаровской государственной академии экономики и права

КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В КРЕДИТНЫХ ОРГАНИЗАЦИЯХ

The 21 century is the age of information technologies and it comes with new threats. Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and trojan horses are a few common examples of software attacks.

Keywords: *cybercrime, viruses, banks, hackers, Tyupkin, Carbanak, information security.*

Модель дистанционного банковского обслуживания максимально пытается облегчить работу клиента, но с улучшением качества обслуживания появляются новые риски. Основные проблемы, с которыми сталкиваются участники национальной платёжной системы России, являются вопросы защиты клиентов от киберпреступлений, разработка и создание новых технологий, взаимодействие в сфере обмена информацией между финансовыми институтами и клиентами, ранее не работавшими с электронными средствами (пенсионеры, молодые люди, малограмотное население) [2, с. 112].

Согласно данным «Глобального исследования рынка программного обеспечения» за 2014 г., в России уровень нелицензионного программного обеспечения составляет 62 %. Хотя данный показатель снизился с 83 % начиная с 2005 г., он по-прежнему остаётся одним из самых высоких в мире. Зачастую в пиратском программном обеспечении содержатся вредоносные программы, которые, в свою очередь, могут способствовать краже личных данных [4].

Сейчас стали популярны «фишинг-атаки», суть которых в том, чтобы перенаправить пользователя на поддельный сайт. Таким образом, если компьютер пользователя инфицирован данным вирусом, то, пытаясь зайти на сайт своего банка для оплаты услуг, он будет перенаправлен на поддельный сайт кредитной организации, интерфейс которого практически идентичен оригиналу, где пользователь компьютера, ничего не подозревая, вводил все свои необходимые для платежа данные. Платёж совершался, но деньги поступали на счёт преступника. Возможен и другой сценарий, когда непосред-

ственно фишинговый сайт находится в сети и предлагает какую-либо услугу.

Одна из наиболее известных событий в истории фишинговых атак, произошла в 2014 году. Мошеннический сайт предлагал купить посетителям электронный билет на чемпионат мира по футболу. Футбольный фанат заполнял форму для оплаты, то есть вводил всю личную информацию о себе, после чего появлялось уведомление о том, что платёж проведён, и необходимо скачать и распечатать электронный билет. На самом деле происходило следующее: пользователь скачивал троянский вирус к себе на компьютер, который перехватывал всю имеющуюся информацию, по большей части финансового характера, и отправлял злоумышленнику [9]. Популярным методом дистанционного обслуживания клиентов являются банкоматы. Банкомат, в свою очередь, представляет собой компьютер в защитном боксе, с ячейками для денег. Злоумышленники не могли обойти стороной и его. Для использования банкомата необходимо вставить карту в банкомат и ввести пин-код.

Широкое распространение по краже средств из банкоматов получил скимминг, то есть физическая подмена специальных устройств банкомата. Например, на отверстие для ввода карточки и на клавиатуру банкомата, накладывается специальное скимминговое оборудование, копирующее данные магнитной полосы и записывающее PIN-код, которое внешне практически невозможно отличить от оригинального вида. После проведённых махинаций, злоумышленник переписывает данные владельца на фальшивую карту и снимает со счёта клиента имеющиеся деньги. Как уже было сказано выше, банкомат – компьютер, значит, на него возможно повлиять при помощи вирусного программного обеспечения.

В октябре 2014 г. «Лаборатория Касперского» опубликовала отчёт о криминалистическом расследовании грабежа банкоматов. Данная процедура помогла выявить более 50 заражённых банкоматов восточноевропейских банков. Из 50 обнаруженных банкоматов, 20 было выявлено в России, что свидетельствует о том, что именно российские банкоматы были основной целью преступников [8].

Процесс заражения банкоматов вирусом выражался в следующем: злоумышленник открывал ключом верхнюю часть банкомата, затем устанавливал троянский вирус «Tyupkin» при помощи диска. Момент несанкционированного проникновения был записан на камеру видеонаблюдения. После установления вредоносного программного обеспечения отключалась антивирусная система, установленная на банкомате. Сложность обнаружения вируса была обусловлена его нахождением «в спячке», то есть большую часть недели вирус никак не влиял на работу банкомата, а только по ночам с субботы на воскресенье и с воскресенья на понедельник включал на банкомате функцию ввода дополнительной команды. Злоумышленник приходил к заражённому банкомату и вводил определенную комбинацию на клавиатуре банкомата, после чего получал доступ в секретное командное меню, из которого мог или начать процесс выемки денег, или производить операции с самим вирусом, в том числе удалить его

из памяти. Для того чтобы извлечь деньги, злоумышленнику нужно знать не только код соответствующей команды, но и специальную формулу, по которой рассчитывается одноразовый сессионный ключ. Если команда и одноразовый код были введены верно, программа предлагала выбрать кассету, в которой хранятся деньги, и произвести выдачу наличных средств в виде 40 купюр определённого достоинства. Обнадёживающим фактором в данной ситуации выступает то, что преступники научились взламывать аппараты лишь одного производителя, и, если банки не хотят терять деньги, им необходимо позаботиться о физической защите своих банкоматов.Тем самым с целью минимизации риска необходимо усилить инвестирование денежных средств в защитные решения, вплоть до установки сигнализаций. В феврале 2015 г. был опубликован отчёт совместного расследования «Интерпол», «Европол» и «Лаборатория Касперского», раскрывший беспрецедентную киберпреступную операцию, длившуюся два года, в рамках которой злоумышленники похитили около миллиарда долларов США. От деятельности злоумышленников пострадали около 100 банков, платёжных систем и других финансовых организаций из почти 30 стран, в частности России, США, Германии, Китая, Украины, Канады, Гонконга, Тайваня, Румынии, Франции, Испании, Норвегии, Индии, Великобритании, Польши, Пакистана, Непала, Марокко, Исландии, Ирландии, Чехии, Швейцарии, Бразилии, Болгарии и Австралии [5].

Такая хакерская группировка получила название «Carbanak», является международной и включает киберпреступников из России, Украины, ряда других европейских стран, а также Китая. Она использовала методы, характерные для целевых атак. Основное отличие от многих других ограблений заключается в том, что киберпреступники похищали деньги напрямую у банков, а не у пользователей.

Полностью процедура от заражения первого компьютера и до сокрытия следов преступления занимала в среднем от двух до четырех месяцев на один банк. За такой рейд киберпреступники крали до 10 млн долларов. По официальным данным, похищенная сумма составила 300 млн долларов, но эксперты полагают, что данная сумма около 1 млрд долларов. Особенность ограбления состояла в том, что хакеры не зависели от используемого банком программного обеспечения, даже если у банка оно было уникальным. Преступники не взламывали банковские сервисы, они проникали в корпоративную сеть и тем самым все их действия не вызывали подозрений. Киберпреступники попадали в банковскую сеть через электронные письма, которые рассылались сотням банковских служащих, которые заведомо содержали в себе вирус «Carbanak». После того как был заражён один из компьютеров, хакеры находили компьютеры администраторов систем денежных транзакций и разворачивали видеонаблюдение за их экранами. Таким образом, банда «Carbanak» знала каждую деталь в работе персонала банка и могла имитировать привычные действия сотрудников при переводе денег на мошеннические счета. Процесс кражи денег группировкой «Carbanak» проходил следующим образом.

1. Для снятия денег киберпреступники использовали онлайн-банкинг или платёжные системы для перевода денежных средств со счёта банка на свои счета, которые были открыты в банках Китая и Америки.

2. Выявлены случаи, когда хакеры проникали в систему бухгалтерского учёта и при помощи мошеннических транзакций «раздували» баланс средств на счёте, то есть киберпреступники узнавали, что на счёте находится 3 тысячи дол., тогда они увеличивали баланс до 10 тысяч и переводили 7 тысяч себе. Владелец счёта ничего не узнавал о данных транзакциях, поскольку деньги его оставались на месте.

3. Помимо всего прочего, киберграбители получали контроль над банкоматами и активировали команды на выдачу наличных в установленное время. После этого к банкомату подходил кто-нибудь из членов банды и забирал деньги.

Переходя непосредственно к вопросу об угрозе внутреннего инфицирования банковских компьютеров вредоносным программным обеспечением, стоит отметить случай обнаружения уникального вируса. Хакерская профессиональная группа «EquationGroup», ведет свою деятельность на протяжении почти двадцати лет, и ее действия затронули тысячи, а возможно, и десятки тысяч пользователей в более чем 30 странах мира. Ниболее пострадавшими называются Иран, Россия, Пакистан, Афганистан, Китай, Мали, Сирия, Йемен и Алжир [6].

Данная преступная организация привнесла новаторские разработки в области вредоносного программного обеспечения. К примеру, в заявлении «Лаборатории Касперского» сказано, что впервые в своей практике обнаружены модули, которые позволяют перепрограммировать операционную систему жёстких дисков 12 основных производителей, WesternDigital, SeagateTechnology, Toshiba, IBM, MicronTechnology и SamsungElectronics. Таким образом, злоумышленники добиваются двух целей: во-первых, однажды попав в операционную систему жёсткого диска, вредоносное программное обеспечение остаётся там навсегда – его невозможно ни обнаружить, ни избавиться от него, оно не может быть удалено даже в случае форматирования диска. Во-вторых, у атакующих есть возможность создать себе «тихую гавань» в виде секретного хранилища, где может безопасно собираться вся необходимая информация [7].

Таким образом жёсткие диски, используемые на данный момент в кредитных организациях, потенциальная угроза, поскольку неизвестно, как в будущем проявит себя вирус, возможно, он уже сейчас собирает необходимую информацию для вывода к киберпреступникам.

Подводя итог, хотелось бы отметить несколько важных моментов как для собственной информационной защиты как для клиентов банков, так и непосредственно для кредитных организаций.

Для клиентов банка в первую очередь необходимо при использовании дистанционного банковского обслуживания быть предельно внимательными, обращать внимание на необычные детали. Если замечено отклонение от нормы, то необходимо сообщить в банк или полицию. Во-вторых, клиентам, с целью защи-

ты личных данных, следует использовать антивирусное программное обеспечение, а также устанавливать программы на свой компьютер только с проверенных источников. С целью минимизации банковских рисков, кредитным организациям необходимо усилить внутренний контроль за автоматизированными информационными системами и техническими средствами, увеличить инвестиции в собственную безопасность [3, с. 31]. Наряду с этим, необходимо обратить внимание на уровень физической защиты банкоматов, а также проверять лица, имеющие доступ к ним, чтобы исключить проникновение преступников. Кроме того, важно укреплять сотрудничество с передовыми агентствами защиты информационной безопасности.

В связи со случаями обнаружения скрытых вирусов на жёстких дисках иностранного изготовителя, рекомендуем развивать собственное импортозамещающее производство комплектующих изделий для компьютеров.

Список использованных источников

1. Об информации, информационных технологиях и о защите информации : ФЗ 27.07.2006 г. № 149-ФЗ (в ред. от 21.07.2014 г.).

2. Пономарёва Н. А. О необходимости повышения финансовой грамотности / Н. А. Пономарёва, Л. В. Масюкова. Хабаровск : РИЦ ХГАЭП, 2013. 110 с.

3. Пономарёва Н. А. Внутренний контроль и аудит в кредитной организации / Н. А. Пономарёва, Л. В. Масюкова. Хабаровск : РИЦ ХГАЭП, 2014. 180 с.

4. Как снизить уровень нелицензионного ПО в России. – URL : http://www.cnews.ru/reviews/?2014/12/17/590962 (дата обращения: 12.03.2015).

5. Ограбление XXI века : хакерам удалось украсть $1 млрд. – URL : http://blog.kaspersky.ru/billion-dollar-apt-carbanak/6950/ (дата обращения: 15.03.2015).

6. «Касперский» выявил американский шпионский вирус для жестких дисков. URL: http://most.tv/news/39596.html (дата обращения: 15.03.2015).

7. «Лаборатория Касперского» раскрыла американский шпионский вирус. URL:https://hi-tech.mail.ru/news/equation-group.html (дата обращения: 15.03.2015).

8. Как вирус «Тюпкин» грабит банкоматы. – URL : http://www.banki.ru/news/daytheme/?id=7213033 (дата обращения: 15.03.2015).

9. Почему работает фишинг и как с ним бороться. – URL : http://blog.kaspersky.ru/how-to-avoid-phishing/5411/ (дата обращения: 15.03.2015).