Антон СВИНЦИЦКИЙ
руководитель отдела консалтинга АО «ДиалогНаука»

Виктор СЕРДЮК
генеральный директор АО «ДиалогНаука»

ОСНОВНЫЕ ВЕКТОРЫ АТАК НА БАНКИ

СОВРЕМЕННЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

На сегодняшний день банки все чаще становятся мишенью для атак со стороны злоумышленников, поскольку проникновение в автоматизированные системы банка позволяет нарушителям получить прямой доступ к финансовым ресурсам. Именно поэтому банковская сфера одной из первых попала в лидеры по количеству целенаправленных атак и уровню понесенного ущерба, который в реальности может превышать официальные данные в разы. В рамках данной статьи будут рассмотрены основные векторы для потенциальных атак на кредитно-финансовые организации, а также возможные пути защиты от них.

АТАКИ НА АБС

Для проникновения в корпоративную сеть банка и последующего получения доступа к АБС злоумышленники чаще всего используют два вектора атак — это рассылка фишинговых сообщений электронной почты с вредоносным содержимым либо привлечение банковских сотрудников на сайты с вредоносным содержимым или фишинговым интерфейсом, имитирующим внутренние системы банка. В обоих случаях важным элементом проникновения внутрь корпоративной сети является преодоление периметровых средств защиты. Для этого используются специальные вредоносные программы, которые оптимизированы для преодоления стандартных средств защиты, таких как антивирусы и системы обнаружения атак.

Отличительной особенностью таких целенаправленных атак (APT) является постоянное совершенствование методов атаки, адресность используемых экземпляров вредоносного кода и контролируемость самого процесса атаки с последующим уничтожением следов проникновения. В современных условиях это означает использование сложных методов упаковки вредоносных программ, адресный фишинг, который сложно отличить от легитимного информационного ресурса или письма, скрытые протоколы коммуникации между злоумышленником и инфицированными компьютерами и, в результате, длительный период присутствия нарушителя в системе. Так, по данным компании Hewlett Packard Enterprise, среднее время между проникновением злоумышленников в систему и их обнаружением составляет 243 дня, то есть практически 8 месяцев.

Основными инструментами для защиты от целенаправленных атак являются средства углубленного анализа передаваемых файлов с возможностью их запуска в виртуальных машинах — этот инструмент в простонародье называется «песочница» (sandbox). Она позволяет обнаруживать хорошо замаскированные вредоносные программы и блокировать их дальнейшее распространение в корпоративной сети банка. Одним из примеров такого рода систем является решение FireEye, которое хорошо зарекомендовало себя в ряде ведущих российских банков.

Еще одним инструментом защиты являются системы обработки и корреляции событий информационной безопасности (SIEM). Правда, для ее эффективного функционирования требуется установка и правильная настройка правил корреляции, а также наличие внедренных процессов управления инцидентами безопасности. При этом для расширения возможностей SIEM-систем необходимо использовать различные классы средств защиты информации, которые будут являться поставщиками событий безопасности, например, системы выявления аномалий в поведении пользователей (UEBA). Интеграция с UEBA позволяет выявлять нелегитимное использование учетных записей пользователей злоумышленниками, получившими доступ к АБС путем перехвата идентификационной и аутентификационной информации. В большинстве случаев поведение такого пользователя будет сильно отличаться от будничных действий обычного сотрудника или пользователя, назначенного на такую же роль в АБС.

АТАКИ НА СИСТЕМЫ ДБО

Если собственную информационную систему банк еще может контролировать, то защиту клиента обеспечить значительно сложнее. Поэтому часто целенаправленные атаки организуются не на сам банк, а на его клиентов. Здесь могут использоваться целенаправленный фишинг якобы от имени банка, фальшивые мобильные приложения, вредоносные модули браузера, перенаправляющие запросы пользователя на подставные сайты, и многое другое.

Системы ДБО в вопросах обеспечения безопасности финансовых транзакций очень сильно зависят от трех аспектов: доверенной аутентификации клиента и подтверждения проводимых операций, безопасной среды исполнения приложения и защищенного канала взаимодействия между системой клиента и банком в рамках системы ДБО. Хакеры могут целенаправленно атаковать все три элемента. Например, для получения паролей от веб-приложения создать фиктивный интерфейс банка и послать на него ссылку клиентам или для атаки на коммуникационную составляющую внедрить в браузер модуль, который будет перенаправлять запросы на специальный посреднический сайт злоумышленников. При заражении вредоносной программой рабочей станции, с которой происходит взаимодействие с системой ДБО, злоумышленники могут перехватывать весь трафик и подменять реквизиты платежей.

Для каждого из трех указанных ключевых компонентов разработаны средства противодействия целенаправленным мошенническим действиям. Для защиты аутентификации — одноразовые пароли, средства двухфакторной аутентификации или аппаратные устройства с электронной подписью документов. Для защиты от вредоносного кода — антивирусы с встроенными функциями контроля поведения приложений (HIPS). Для защиты коммуникаций — взаимная аутентификация сторон и шифрование канала связи между клиентским приложением и сервером банка, например, с помощью TLS. Однако целенаправленные атаки характерны тем, что стандартные методы могут не сработать, поэтому банк должен также контролировать логику происходящих событий с помощью систем защиты от мошенничества или антифрод-систем, адаптированных под требования банка. Такие системы позволяют обнаруживать аномальное поведение клиентов и блокировать подозрительные транзакции. В ряде случаев есть возможность создавать антифрод-системы на базе уже установленных в банке SIEM-систем. Так, например, такая возможность есть у продуктов HPE ArcSight, на базе которых можно создать дополнительный набор правил корреляции и отчетов, выявляющих признаки мошенничества в банковских транзакциях.

ПО ДАННЫМ КОМПАНИИ HEWLETT PACKARD ENTERPRISE, СРЕДНЕЕ ВРЕМЯ МЕЖДУ ПРОНИКНОВЕНИЕМ ЗЛОУМЫШЛЕННИКОВ В СИСТЕМУ И ИХ ОБНАРУЖЕНИЕМ СОСТАВЛЯЕТ 243 ДНЯ, ТО ЕСТЬ ПРАКТИЧЕСКИ 8 МЕСЯЦЕВ

АТАКИ НА СИСТЕМЫ МЕЖБАНКОВСКОГО ОБМЕНА

Переводы денежных средств осуществляются как с помощью платежных систем, таких как Visa, MasterCard или НСПК, так и с помощью системы межбанковских расчетов SWIFT и/или Банка России. В данном случае атака может быть направлена на подделку реквизитов платежей в транзакции или поручении, чтобы деньги были переведены не на счет требуемого получателя, а на счет злоумышленника. Так, например, в этом году была опубликована информация об успешной атаке на SWIFT, в результате которой злоумышленникам удалось похитить средства национального банка Бангладеш на десятки миллионов долларов. К сожалению, успешные атаки на АРМ КБР (автоматизированное рабочее место клиента Банка России) также не являются редкостью. Именно поэтому Банк России выпустил целый ряд документов, направленных на повышение уровня защиты кредитно-финансовых организаций от такого рода атак, в частности Положение Банка России от 24 августа 2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России». Для защиты данных платежных карт клиентов банков активно используется международный стандарт PCI DSS, который является обязательным для банков, обрабатывающих карточные данные, в том числе, имеющие собственные процессинговые центры.

АТАКИ НА БАНКОМАТНЫЕ СЕТИ

Еще одним вектором для потенциальных атак злоумышленников являются банкоматные сети. По сути, современный банкомат представляет собой тот же компьютер, подключенный к сети банка. При этом в качестве операционной системы чаще всего используется общесистемное ПО Microsoft Windows, в том числе Windows XP, а также, в силу аппаратных и/или программных ограничений, не используются даже простейшие средства защиты информации — антивирусы и средства мониторинга. Злоумышленник может атаковать банкомат посредством как локального, так и удаленного доступа, используя уязвимости в общесистемном и прикладном ПО банкомата. Для защиты от такого рода угроз необходимо использовать специализированные средства защиты, предназначенные для защиты самого банкомата, а также каналов взаимодействия между ним и корпоративной сетью банка.

* * *

В настоящее время существует достаточно большое количество векторов, по которым злоумышленник может атаковать банк. Для эффективной защиты от такого рода угроз необходимо использовать комплексный подход, предусматривающий применение как организационных, так и технических мер защиты. Именно такой подход предусмотрен в положениях нового ГОСТа по защите информации, разработанного Центральным банком России, принятие которого ожидается в текущем году.