УДК 336.719.2

ЗАЩИТА УСТРОЙСТВ САМООБСЛУЖИВАНИЯ ОТ АТАК С ПРИМЕНЕНИЕМ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Воробьёв Станислав Юрьевич, начальник сектора информационной безопасности управления безопасности ЗАО «РРБ-Банк»
Vorobyov Stanislav Yurievich, Master of Technical Sciences, Head of the Information Security Sector of the Security Department of RRB-Bank CJSC, vorobyovsy@rrbbank.by
Мишнев Григорий Викторович, заместитель начальника отдела **Генеральной прокуратуры Республики Беларусь**
Mishnev Grigory Viktorovich, Deputy Head of the Department of the General Prosecutor's Office of the Republic of Belarus, g.mishnev2015@gmail.com

Аннотация. В статье обосновывается стабильность кредитно-финансовой сферы, как составной части национальной безопасности государства, угрозы банковским учреждениям при помощи средств высоких технологий, необходимость применения антивирусного программного обеспечения на терминальном оборудовании (банкоматах, инфокиосках и пр.)

Ключевые слова. банк, банкомат, информационная безопасность, антивирус, вредоносное программное обеспечение

Одними из наиболее существенных угроз национальной безопасности государства являются угрозы в экономической и информационной сферах. Противоправная деятельность злоумышленников в киберпространстве, направленная в отношении информационной инфраструктуры банков,

которая основывается на использовании современных информационных систем и технологий, может привести к дестабилизации финансовой и денежно-кредитной систем государства.

В каждом банке функционирует собственная служба безопасности (в том числе информационной). Многие сертифицируют свои процессы в соответствии с требованиями международных стандартов в сфере информационной безопасности таких как PCI DSS, ISO 27001, Программа безопасности пользователей SWIFT и т.д. Применение в информационных системах банковских учреждений защитных мероприятий по тщательному отбору персонала, поддержанию здорового климата в коллективе, ролевой модели доступа пользователей, эксплуатации антивирусного программного обеспечения, а также DLP-систем и SIEM-систем, брандмауэров, разработке локальных актов по вопросам информационной безопасности в совокупности существенно снижает вероятность успешной реализации таргетированной кибератаки злоумышленников.

Вместе с тем в банковской деятельности широко применяются банкоматы, информационные платежные терминалы самообслуживания, электронные депозитарные машины (т.н. терминальное оборудование). Одновременно за последние несколько лет произошла эволюция от физических атак на терминальное оборудование до атак с применением средств высоких технологий. Так, согласно данным за 2018 год, представленным Банком России в Обзоре несанкционированных переводов денежных средств, были зафиксированы следующие способы воздействия на банкоматы:

- физическое воздействие на банкомат, платежный терминал (взрыв, взлом и т.д.);
- удаленное управление банкоматом, платежным терминалом, в том числе вследствие заражения вредоносным кодом;
- прямое подключение к банкомату технических устройств, позволяющих им управлять[1].

Для логического завершения кибератаки на банкомат необходимо находиться рядом с последним для изъятия наличных денежных средств. Как правило, для непосредственного обналичивания денег с атакованного банкомата злоумышленники привлекают «мулов» - пособников, которые по команде вводят уникальный сессионный ключ либо используют специальную карту для авторизации несанкционированной транзакции, после чего изымают наличность[2].

Однако, до финальной стадии необходимо осуществить внедрение вредоносного программного обеспечения в компьютер банкомата, что производится получением физического доступа к USB-портам либо оптическому приводу последнего, либо удаленным внедрением вредоносного программного обеспечения (далее - ВПО), посредством предварительной компрометации внутренней информационной сети банка, получением и дальнейшим распространением зловреда на сеть банкоматов.

Вышеуказанные инциденты с терминальным оборудованием крайне негативно сказываются на репутации кредитно-финансовых учреждений[3]. Последним необходимо применять нижеперечисленные меры на терминальном оборудовании для противодействия подобным атакам:

- терминальное оборудование должно работать под управлением актуальных версий операционной системы с установленными последними обновлениями безопасности;
- отключить все неиспользуемые системные службы и приложения, чтобы устранить дополнительные векторы атаки;
- обеспечить надежное шифрование соединения между терминальным оборудованием и хостом;
- исключить возможность подключения неавторизованных внешних USB-накопителей;
- терминальное оборудование не должно располагаться в одной сети с рабочими станциями сотрудников;
- организовать надежную физическую защиту банкоматов и зон их размещения;
- контролировать и ограничивать доступ сотрудников сервисных организаций, обслуживающих банкоматную сеть;
- проводить регулярное обучение по противодействию актуальным угрозам для сотрудников, задействованных в процессах обслуживания и мониторинга работы банкоматов;
- организовать онлайн-мониторинг банкоматной сети как в части работоспособности банкоматов и непрерывности операций, так и состояния кибербезопасности.

Надежным классическим способом защиты от атак с использованием ВПО является применение лицензионного антивирусного программного обеспечения (далее - антивирусы). Антивирусы

могут легко найти ВПО в информационной системе, но крайне важно поддерживать антивирусы обновленными.

Необходимо сакцентировать внимание на отсутствие в (технических) нормативных правовых актах, регулирующих сферу информационной безопасности в банковской отрасли Республики Беларусь (государственный стандарт Республики Беларусь «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения» (далее - СТБ 34.101.41-2013) и нормативный правовой акт Национального банка Республики Беларусь, регулирующий сферу обеспечения информационной безопасности банков Республики Беларусь «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения и терминология» (далее - ТТП ИБ 1.1-2020)) прямого нормативного предписания на обеспечение антивирусной защиты терминального оборудования (обязательной антивирусной защите подлежат только сервера и рабочие станции), что существенно увеличивает риск заражения терминального оборудования в случае атак с использованием ВПО.

Так, согласно абз.1 п. 7.5.1 СТБ 34.101.41-2013 «На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты, сертифицированные в национальной системе сертификации либо имеющие положительное заключение государственной экспертизы»3. Таким образом, прямое требование по установке антивирусного программного обеспечения на терминальное оборудование в вышеуказанном СТБ отсутствует (установка антивируса фактически осуществляется банками–владельцами терминального оборудования «инициативно»). Абз.1 п. 7.5.1 ТТП ИБ 1.1-2020 фактически дублирует требование стандарта «на всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, должны применяться средства антивирусной защиты»[4].

На основании вышеизложенного представляется целесообразным в данных СТБ и ТТП дополнить абз. 1 п.7.5.1 словами «а также терминальном оборудовании» изложив его в следующей редакции: «На всех автоматизированных рабочих местах и серверах автоматизированной банковской системы, если иное не предусмотрено технологическим процессом, а также терминальном оборудовании (банкоматах, платежно-справочных терминалах самообслуживания, электронных депозитарных машинах) должны применяться средства антивирусной защиты».

Вместе с тем для придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, требуется внесение изменений в Банковский кодекс Республики Беларусь[5].

Вышеуказанные изменения закрепят необходимость обязательного применения средств антивирусной защиты и, как следствие, повысят эффективность мероприятий по обеспечению и поддержанию кибербезопасности в банковской сфере, позволят предотвратить и (или) снизить ущерб от киберинцидентов, повысят стабильность функционирования как отдельных банков, и, как следствие, стабильность функционирования всей банковской сферы государства в целом.

На основании вышеизложенного представляется возможным сделать вывод, что для эффективной защиты банковского терминального оборудования и противодействия атакам с применением ВПО необходимо осуществление комплекса мероприятий, как нормативно-правового, так и инженерно-технического характера.

Список использованных источников

1. Кибербезопасность в условиях электронного банкинга: Практическое пособие / Под ред. П.В. Ревенкова. – М.: Прометей, 2020. – 522 с.

2. Торчиков, В. 10 лет изящного взлома. Как развивалось вредоносное ПО для банкоматов / В. Торчиков // Журн. «Системы безопасности». – 2019. – № 5. – С. 32-36.

3. Защита банкоматов и платежных терминалов от вредоносных программ и инсайдеров [Электронный ресурс] // Издание Anti-Malware.ru – Независимый информационно-аналитический центр по информационной безопасности. Режим доступа : https://www.anti-malware.ru/node/2354. – Дата доступа : 12.03.2022.

4. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А.И. Белоус, В.А. Солодуха. – Москва ; Вологда : Инфра-Инженерия, 2020. – 692 с.

5. Концепция обеспечения кибербезопасности в банковской сфере [Электронный ресурс] // Официальный сайт Национального банка Республики Беларусь. Режим доступа : https://www.nbrb.by/legislation/informationsecurity. – Дата доступа : 12.03.2022.