Николай ПЕТРОВ
Заместитель
генерального директора
АО «ДиалогНаука», CISSP

ЗАЩИТА БАНКОВ ОТ НЕЗАКОННОГО ВЫВОДА ДЕНЕЖНЫХ СРЕДСТВ

Рекомендации по информационной безопасности

Банки регулярно теряют деньги в результате успешных атак злоумышленников. Так в марте 2016 Металлинвестбанк опубликовал пресс-релиз о похищении хакерами средств с его корреспондентского счета в Центробанке. 29 февраля 2016 года Металлинвестбанком была пресечена попытка хищения средств неустановленными лицами в результате хакерской атаки путем их вывода с корреспондентского счета в Центральном банке в сумме около 667 млн рублей. Потери банка от этой атаки составили 200 млн рублей. Остальные денежные средства удалось заблокировать и вернуть. Из-за этой атаки банк просил ЦБ отключить его от системы банковских электронных срочных платежей (БЭСП).

Система банковских электронных срочных платежей (БЭСП) Банка России введена ЦБ для расчетов в режиме реального времени для проведения срочных платежей в рублях. Сообщения БЭСП отправляются и обрабатываются сразу, в реальном времени.

В январе 2016 года, Русский Международный Банк подвергся хакерской атаке, и обратился к ЦБ с просьбой отключить его от системы БЭСП. Со слов представителей банка, мошенники произвели несколько тысяч списаний денежных средств с корсчетов банка в адрес примерно 60 других кредитных организаций, затем эти деньги были перечислены, в основном физлицам. Когда в банке получили первую выписку из ЦБ в 10 часов утра, то увидели нехарактерную активность по счетам.

В декабре 2015 года, подобный случай произошел в Казанском Алтынбанке. По заявлению председателя правления банка Рината Абдуллина, хакеры в ходе атаки попытались похитить 60 млн рублей. Способ хищения был следующий: в компьютерную сеть банка была внедрена специальная программа, которая подменила в платежных поручениях клиентов наименования получателя денежных средств и их банковские реквизиты. Денежные средства были отправлены в два крупных московских банка на счета юридических лиц. Затем со счетов этих юридических лиц деньги были перечислены на счета еще двух десятков организаций, находящихся в различных регионах России и в разных банках.

Это несколько известных случаев за 3 месяца. Значит, **несанкционированный вывод денежных средств из банков происходит регулярно**. Это происходит потому, что злоумышленники используют специальные вредоносное программное обеспечение и уязвимости нулевого дня.

0day (англ. zero day) — термин, обозначающий не устранённые уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы.

Это позволяет злоумышленникам обходить традиционные средства защиты: антивирусы, межсетевые экраны, включая межсетевые экраны нового поколения, системы обнаружения и предотвращения вторжений, шлюзы веб-безопасности.

Я хотел бы поделиться нашим опытом. За последние несколько лет мы провели десятки пилотных проектов и внедрений решений для защиты от атак нулевого дня. Практически в каждом пилотном проекте мы обнаруживали внутри корпоративной сети персональные компьютеры, управляемые извне.

Иными словами, злоумышленники могли получать любой доступ к информации на этих компьютерах, читать и копировать документы и электронную почту, знать все пароли пользователя.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ:

Разработать и внедрить «Регламент реагирования на инциденты в области информационной безопасности». Регламент должен включать в себя:

- Определение ролей и ответственности;
- Описание типовых сценариев инцидентов;
- Разработку программы действий в случае возникновения инцидентов;
- Обучение персонала методам реагирования по фактам нарушения информационной безопасности.

Как минимум, ограничить доступ к рабочим местам АРМ КБР и БЭСП со стороны устройств, имеющих доступ к сети Интернет. Это существенно затруднит атаку, сделав ее практически невозможной.

В случае невозможности такого ограничения, установить специализированную систему защиты от атак нулевого дня, принимая во внимание следующие факторы:

- Поддержка операционных систем, используемых сотрудниками банка, например, Microsoft Windows, Mac OS X, мобильные операционные системы iOS и Google Android;
- Контроль каналов распространения вредоносного ПО: Web, e-mail, CD, DVD, USB и др.;
- Собственная система виртуализации для выявления признаков вредоносной активности. В противном случае вредоносный код будет понимать, что он запущен в виртуальной среде и не будет производить никаких действий;
- Предотвращение распространения атаки. При проникновении вредоносного кода на рабочие места сотрудников, принудительная изоляция администратором безопасности пострадавших рабочих мест от доступа к компьютерной сети.