Как изменился характер кибер-атак на банки за последнее время

Фото: НТЦ «Вулкан»

За последнее время характер кибер-атак на банковский сектор изменился: теперь преступники нацелены не только на клиентов, но и на сами финансовые институты — действительно, зачем красть по частям и мало, когда можно за один раз и много? Давайте вместе взглянем на новые тенденции в проведении таких атак

Текст: **АННА МАКСИМОВА,** ЭКСПЕРТ ОТДЕЛА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НТЦ «ВУЛКАН»

Направленные атаки

Отчеты известных компаний пестрят сообщениями о том, что теперь все атаки на банки являются направленными: при осуществлении таких атак злоумышленники не просто заранее выбирают свою жертву, но и тщательно ее изучают (похоже, девиз know your client находит отражение и в «работе» кибер-преступников). Для осуществления успешного проникновения в банковскую систему кибер-преступники активно используют социальную инженерию, фишинговые письма и известные уязвимости стандартного программного обеспечения.

Социальная инженерия + фишинговое письмо + известная уязвимость стандартного ПО = успешное проникновение в систему

Правдоподобность фишинговых писем поражает: изображения, содержащиеся в письмах, загружаются с официальных ресурсов, а особенности целевой аудитории прорабатываются с особой тщательностью, так, менеджеры получают письма о новых законодательных требованиях от «Банка России», бухгалтера — счета и договора на «государственные контракты», менеджеры по работе с клиентами — письма от «действующих» и «потенциальных клиентов».

Наблюдай и учись

При проведении кибер-атак злоумышленники все чаще используют методы, применяемые в APT-атаках: они стараются максимально слиться с IT-инфраструктурой банка и как можно дольше оставаться незамеченными, наблюдая и выжидая.

Скрытность злоумышленников обеспечивается активным использованием модифицированных версий легальных программ (например, Remote Manipulator System для удаленного управления компьютером, Mimikatz для получения паролей, Punto Switcher в качестве keylogger'а), а также общедоступных кодов вредоносных программ типа Carberp, Zeus, SpyEye. Во многих случаях преступники используют инструменты шифрования, за счет чего взаимодействие между компьютером жертвы и CnC-сервером злоумышленников остается недетектируемым программами-анализаторами трафика.

Во время пребывания внутри банковской сети кибер-преступники не просто наблюдают за действиями пользователя, но и обучаются премудростям работы со специальным банковским ПО: все действия банковского работника записываются на видео, которое в дальнейшем отсылается на CnC-сервер злоумышленников и используется для обучения и вывода денежных средств.

Полный скрытный контроль над банковской системой, а также полученные в процессе «онлайн-обучения» навыки позволяют преступникам осуществлять вывод денег различными способами, максимально приближенными к легальным операциям:

– удаленная отправка команды банкоматам на выдачу наличных;

– осуществление денежных переводов со счетов клиентов;

– манипулирование системами онлайн-банкинга для скрытого осуществления денежных переводов.

Вместо заключения

Злоумышленники учатся и развиваются, применяют все новые техники и технологии, что ставит перед ИБ-специалистами задачи не просто реагирования, но адаптации к видоизменяющемуся ландшафту кибер-угроз.

Безусловно, в силу скрытного характера действий злоумышленников о многих атаках мы узнаем много позже. Возможно, и за вами уже наблюдают, просто вы пока об этом не знаете. Б.О