Идейный кибертерроризм: банки под ударом

Кибервойны представляют опасность не только для отдельных стран и политических организаций. Концепция, всего десятилетие назад казавшаяся теоретической, сейчас таит угрозу для обычных людей и бизнеса любого уровня. Один из таких примеров — вступившая уже в четвертую фазу атака группы Кибервоинов Изза ад-Дина аль-Кассама на североамериканские банки. Группировка, по словам ее активистов, совершает DDoS-атаки на финансовые учреждения в знак протеста против размещения в Сети фильма «Невинность мусульман». В своих заявлениях они приводят формулу, по которой определяется сумма, которую должны потерять банки США в зависимости от количества просмотров каждого видео. Средняя стоимость минуты успешной DDoS-атаки, по расчетам активистов, составляет 30 тыс. долл.

Осенью прошлого года были атакованы крупнейшие банки США, такие как JPMorgan Chase & Co и Bank of America. Затем под удар попали банки среднего уровня и некоторые кредитно-финансовые кооперативы, а позже атаки стали проводиться в сочетании с кражей интеллектуальной собственности и финансовым мошенничеством.

Представители атакуемых организаций не комментировали ситуацию, но независимые эксперты сообщали о выходе из строя элементов банковского онлайн-обслуживания. Специалисты считают, что эти атаки направлены из Ирана и являются возмездием за внедрение червя Stuxnet на компьютеры, управляющие центрифугами обогащения урана, что привело к выводу из строя некоторых из них.

Помимо этого преступники используют DDoS-атаки для отвлечения служб безопасности от мошеннических схем и взломов учетных записей. Нередко в компаниях все ответственные за кибербезопасность занимаются одной и той же атакой, не взаимодействуя друг с другом. Киберпреступники же находятся в тесном взаимодействии, так что вредоносный код модернизируется быстрее, чем банки закрывают бреши.

DDoS-атаки могут нанести репутационный ущерб и привести к упущенной выгоде, но в сочетании со взломом учетных записей непосредственный ущерб становится гораздо выше. ИТ-инфраструктура финансовой организации должна защищаться от вторжений в любой ситуации и от любых угроз. Кроме того, необходимо предотвратить угрозы со стороны инсайдеров или взломщиков, получивших доступ к учетным записям системных администраторов.

Надежную защиту информационной системы обеспечивает решение SafenSoft Enterprise Suite. Технологии проактивной защиты позволяют защищать любые части программной среды от модификации вне зависимости от того, использует ли злоумышленник давно известный зловредный код, попавший в базы антивирусов, или применяет угрозу нулевого дня. Кроме того, разделение привилегий и настройка прав доступа к отдельным

Станислав Шевченко, технический директор SafenSoft: «Технологии проактивной защиты, реализованные в продукте SafenSoft Enterprise Suite, обеспечивают высокий уровень безопасности банковских систем».

элементам файловой системы и реестра рабочих компьютеров и серверов помогают передать сотрудникам отдела безопасности непосредственный контроль над действиями пользователей. Инцидент недостаточно предотвратить. При выявлении вредоносной деятельности необходимо проводить расследование, чтобы обнаружить канал атаки и возможное наличие инсайдеров в компании.