УДК 004.05

Социальные сети как вектор атаки для целевых атак

Автор: Еркебай.А.Ғ.
Satbayev University, Казахстан, г.Алматы
Научный руководитель: лектор, Зиро А.А.
Satbayev University, Казахстан, г.Алматы

Аннотация

В данной статье исследованы проблемы обеспечения безопасности в социальных сетях, выявлены уязвимости APT атак с использованием социальных сетей, разработана политика информационной безопасности.

Введение

На сегодняшний день самым уязвимым местом информационной системы является человек. Нарушителю не нужно делать атаки на узлы сетевой инфраструктуры и серверные ресурсы, и проходить firewall (межсетевой экран), ему достаточно использовать социальные сети. С активным развитием социальных сетей все чаще организации внедряют их в свою работу и каждый сотрудник имеет свой аккаунт. Этого достаточно чтобы злоумышленник получил доступ в информационную систему.

Основная часть

Нарушители часто используют методы социальной инженерии для взлома социальных сетей. Очень часто в социальных сетях люди просят помочь в рассылке какой-либо информации. Эта информация может быть вирусным программным обеспечением, которая скрытно внедряется в технические средства. Каждая фотография выложенная в социальных сетях имеет свои метаданные.

В метаданных содержатся:

- Дата и время создания изображения;
- Данные о геолокации;
- Модель камеры и параметры создания снимка (диафрагма, выдержка и т.д.);
- Информация о собственнике снимка.

Каждая социальная сеть имеет свои уязвимости. Например: в социальной сети Вконтакте выставляется на общий доступ все файлы (документы), которые доступны зарегистрированным пользователям данной сети. В социальной сети Whatsapp существует уязвимость, где с помощью специальных инструментов злоумышленник может получить доступ к смартфону, создав документ с расширением gif. В социальной сети Instagram для получения доступа к аккаунтам, нарушитель использует скрипт, который выполняет brute force атаку. В дальнейшем в работе будут разработаны рекомендации для обеспечения безопасности в социальных сетях.