Скрытый майнинг обычно реализуется через заражение браузерным майнером. Одним из вирусов такого типа является JS/CoinMiner, уровень распространенности которого по мнению специалистов компании ESET на сентябрь 2017 года составил 12,45%. Задачей злоумышленника при использовании вируса такого типа является включение зараженного компьютера пользователя в часть распределенной сети, вычислительные мощности которой используются для добычи криптовалюты (Bitcoin, Monero, Zcash и т.п.). Заражению могут быть подвержены не только стационарные компьютеры, но и смартфоны. Основной способ распространения майнинговых скриптов является вредоносная реклама. В наибольшей степени такой вид угрозы актуален для России, Украины и Беларуси из-за выбора языка сайтов, в которые были внедрены скрипты – доменная зона.ru и .by.

Распространение получили также схемы создания фишинговых приложений-кошельков для перехвата закрытых ключей и SEED-фраз; создаются также фишинговые приложения криптовалютных бирж.

Рекомендации по защите от угроз такого типа стандартны: следует выбирать приложения для обмена криптовалют и криптовалютные кошельки аналогично тому, как выбирается для загрузки приложение мобильного банка; при загрузке такого приложения следует убедиться, что оно официальное; при возможности следует использовать двухфакторную аутентификацию для защиты эккаунта криптовалютной биржи/кошелька; своевременно обновлять установленное антивирусное ПО; периодически проверять свое устройство на наличие вирусов.

Литература

1. ESET: криптовалютные мошенники переходят на Android [Электронный ресурс]. – URL: https://www.esetnod32.ru/company/press/center/eset-kriptovalyutnye-moshenniki-perekhodyat-na-android-/. – (дата обращения: 20.04.2018).

2. Компьтеры белорусов используются для тайного майнинга [Электронный ресурс]. – URL: https://42.tut.by/560515/. – (дата обращения: 20.04.2018).

3. Скрытый майнинг на компьютерах белорусов стал массовым [Электронный ресурс]. – URL: https://42.tut.by/577203/. (дата обращения: 20.04.2018).

ОРГАНИЗАЦИЯ БЕЗОПОСНОСТИ БОЛЬШИХ ДАННЫХ

Д.В. Лящук, Н.А. Искров, В.Е. Проволоцкий

Существующие на данный момент подходы к обеспечению защиты технологий больших данных в большинстве своем основаны на использовании точечных мер при отсутствии единой полномасштабной защиты. Сегодня отсутствуют четко сформулированные методы, полностью описывающие шаги и действия по защите больших данных, структурированных и неструктурированных, для которых характерны свои особенности сбора, агрегирования, хранения и анализа. На данный момент можно определить четыре основных направления по защите данных на всех этапах работы с ними.

Первый этап заключается в обеспечении безопасности инфраструктуры. На данном этапе должны применятся лучшие практики по безопасности хранилищ данных и защите вычислений для распределенных программных платформ.

Второй этап защиты – конфиденциальность данных. Сохранение конфиденциальности при обработке и анализе данных, обеспечение безопасности данных, используя криптографические возможности, а также гранулированных контроль доступа к данным помогу наладить безопасность на данном уровне.

Управление данными является третьим этапом защиты. Если существует возможности определения происхождения данных, управления ключами и реализация открытого процесса жизненного цикла данных, аудит использования больших данных, в таком случае можно говорить об успешном выполнении задач данного этапа.

Заключительным шагом к реализации защиты больших данных является целостность данных и процедуры реагирования. На данном этапе будут полезны проверка и фильтрация конечных точек и мониторинг безопасности в режиме реального времени.

Выполнение данных шагов в полном объеме поможет не только избежать

потенциальных проблем в будущем, но и сэкономить достаточно большие средства, что в первую очередь важно для бизнеса.

ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ И ПРОГРАММНАЯ ЗАЩИТА ИНФОРМАЦИИ

А.Н. Макаров, Ю.А. Скудняков

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты для исполнения своих противоправных интересов и получения конфиденциальной информации. Все средства инженерно-технической защиты применяются для различных объектов взаимодействия: людей, информации, финансовых и материальных средств. По назначению средства инженерно-технической защиты делятся на группы: 1) физические средства включают различные средства и сооружения, которые могут препятствовать физическому проникновению или доступу злоумышленников на объекты защиты, к материальным носителям конфиденциальной информации, и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий; 2) аппаратные средства, в которые входит оборудование, содержащее различные приборы, приспособления и устройства, выполняющее функцию защиты информации. На любом предприятии применяется различная аппаратура и системы, которые обеспечивают производственную деятельность. Основной задачей аппаратных средств является обеспечение надежной и уверенной защиты от утечки информации и несанкционированного доступа к ней через технические средства, находящиеся на предприятии; 3) криптографические средства – это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования [1]; 4) программные средства, которые охватывают специальные программы и комплексы, а также информационные системы обработки данных, включающие в себя защиту информации. Приведенные выше средства инженерно-технической и программной защиты являются базовыми для обеспечения защиты информации. В современном мире информационное поле становится основой взаимодействия внутри и между объектами и имеет глобальный доступ по всему миру. Средства защиты находятся в постоянном совершенствовании и развитии для предотвращения доступа в исполнении противоправных действий. Исходя из вышеизложенного, авторами работы разработана система защиты, алгоритм функционирования которой постоянно изменяется и совершенствуется. Только комплексное использование всех групп инженерно-технической и программной защиты позволяет предотвратить несанкционированный доступ к защищаемой информации.

Литература

1. Партыка Т.Л., Попов И.И. Информационная безопасность. М.: ФОРУМ: ИНФРА-М., 2005. 243 с.

ТЕСТИРОВАНИЕ СЕТЕВЫХ РЕСУРСОВ КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

В.В. Маликов, М.А. Бабич, В.Н. Ярошевич

Исследован уровень информационной безопасности (ИБ) сервисов/ресурсов в сети интернет на примере кредитно-финансовых организаций (КФО) Республики Беларусь. Для проведения исследования были выбраны 25 белорусских КФО из реестра Национального банка Республики Беларусь, имеющие специальные разрешения (лицензии) на осуществление банковской деятельности.

На основании проведенного тестирования можно сделать следующие выводы:

1. Наиболее часто используемые AS для КФО: ASN 12406 (ООО «Деловая сеть») – 7 сетевых ресурсов, ASN 6697 (РУП «Белтелеком») – 5 сетевых ресурсов.

2. Структура сервисов/ресурсов ДБО КФО, как правило, имеет уязвимости:

– только 7 (35 %) из 20 КФО не имеют в своей структуре уязвимых referrer-файлов;