Результаты исследований показывают, что при использовании в сети устройства защиты от несанкционированного доступа и его правильной конфигурации удалось оптимизировать работу мультисервисной сети, улучшить ее производительность и обеспечить необходимый уровень безопасности.

Литература

1. Мультисервисные сети следующего поколения [Электронный ресурс]. – URL: http://www.iksmedia.ru/articles/718285-Multiservisnye-seti-sleduyushhego.html (дата обращения: 16.05.2018).

2. Проектирование и моделирование сетей связи в системе Riverbed Modeler / В.Н. Тарасов [и др.]. Самара, 2016. 260 с.

ПОДХОДЫ К ДЕТЕКЦИИ ОБЪЕКТОВ НА ДИНАМИЧЕСКИХ ИЗОБРАЖЕНИЯХ

М.М. Лукашевич

Видеоанатитика в целом и задача детекции объектов на видео в частности являются важными элементами инженерно-технической защиты объектов. Традиционные подходы к детекции объектов на статических или динамических изображениях (видео) включают в себя следующие этапы: сегментация, извлечение признаков и детекция. На этапе сегментации возможно преобразование цветового пространства и применение различных алгоритмов пороговой обработки. В качестве информативных признаков могу использоваться детекторы границ, HOG-признаки, вейвлеты Хаара, Фурье-дескрипторы и др. Детекция и/или распознавание объектов реализуется на базе таких алгоритмов, как SVM классификатор, kNN классификатор, сравнение с эталоном и др.

Типовые схемы не всегда дают требуемую точность детекции. Последние результаты в области глубоких нейронных сетей позволяют улучшить точность детекции объектов. В настоящее время предложено большое число моделей глубоких нейронных сетей. Предложена схема детекции объектов на основе RCNN-детектора [1], состоящего из CNN (сверточной нейронной сети) и классификатора. В частности, предполагается рассмотрение гипотез о метаположении объекта (~2000 К). Гипотезами считаются вырезанные фрагменты изображения, которые подвергаются перемасштабированию. Далее функционирует CNN и вычисляются признаки, на основе которых на следующем этапе выполняется литейная классификация для каждого класса и уточнение местоположения гипотезы. При этом обучается только линейная классификация. Успешность применения глубоких нейронных сетей подтверждена результатами, полученными на массивной базе аннотированных изображений, предназначенной для отработки и тестирования методов распознавания образов и машинного зрения ImageNet [2].

Литература

1. Ross Girshick, Jeff Donahue, Trevor Darrell, Jitendra Malik. Rich feature hierarchies for accurate object detection and semantic segmentation Tech report (v5). 22 Oct. 2016.

2. ImageNet [Электронный ресурс]. – URL: http://image-net.org (дата обращения: 16.05.2018).

МАЙНИНГ КРИПТОВАЛЮТ: НОВЫЕ ВЫЗОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.М. Лыньков, В.С. Князькова

Распространение технологии блокчейн и рост популярности майнинга привели к появлению новых видов угроз информационной безопасности. Сам майнинг представляет собой деятельность по поддержанию работы распределительной сети путем закрытия и создания блоков в технологии блокчейн на основе использования вычислительных мощностей. На данный момент наибольшее распространение получили виды угроз, связанные со скрытым майнингом, а также краже данных криптовалютных кошельков и обменных сервисов.

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