PlayMore

Платформа, объединяющая баскетболистов

Команда

Гинак Валерий

Мандзюк Антон

Чиндин Антон

Case 1. Фишинг и DDOS

Деятельность нашей потенциальной компании, крупного баскетбольного сайта, подразумевает постоянную активность в интернете, а публикуемые нами материалы, в числе которых: новости из баскетбольного мира, различного рода текстовые материалы и тематические статьи, а также платные программы тренировок, реализуемые через партнерские программы, могут стать жертвой различного рода интернет-атак. Самой неприятной и доступной для злоумышленников извне может стать DDOS-атака, которая может привести к полной остановке деятельности серверов нашей сети. Самое неприятное в нем то, что полной защиты от него нет. Если атака достаточно мощная, то сервер будет лежать до тех пор, пока она не прекратится . Данная атака может сопровождаться фишингом, где происходит кража персональных данных пользователя.

Возникшая проблема

Одному из сотрудников нашей компании приходит поддельное письмо на электронную почту от крупной баскетбольной организации, такой как NBA или РФБ с предложением о заключении партнерского соглашения.

Наш сотрудник на радостях переходит на поддельный сайта и вводит туда собственные персональные данные, а также прилагает банковские реквизиты, так как злоумышленники под видом РФБ предлагают ему и нашей организации спонсорство в будущем, так как они якобы заинтересованы в развитии спорта в стране и баскетбола в частности.

Позже произошла транзакция через банк, где были украдены наши и клиентов деньги. Помимо этого, в нашем офисе пропало подключение к сети интернет. Причиной этому была DDOS-атака. Выяснить, что проблема произошла удалось только после остановки постоянного подключения к сети и приглашению сотрудника из обслуживающей компании. Удалось восстановить подключение не сразу, а уровень доверия от клиентов упал, после негативных отзывов на нашем встроенном в сайте форуме и постоянных звонках недовольных .

Методы борьбы

За обеспечение работы нашей сети была ответственна хостинг-компания, и, классифицируя атаку как внешнюю, большую часть ответственности и наших претензий мы направили к данному провайдеру, который обещал утвердить ряд мер. Со своей стороны мы пригласили in-house специалиста, который предложил выполнить оперативные действия в информационной системе, а также разработал ряд профилактических мер.

Методы борьбы

- Создание удаленного ребута и вывода консоли самого сервера на другой ip-адрес по ssh протоколу. Данный метод позволит легко перезагружать сервер, что сможет противостоять первоначальному этапу атаки и отключению сети, что и стало основной проблемой.
- Разработка этапов регулярного обновления программного обеспечения, которые подвергаются исправлению и доработке от самих разработчиков
- Проведение программы настройки сетевых фильтров и антивирусов
- Подключение к облачному сервису, который обеспечивает защиту от ddos-атак от Лаборатории Касперского
- Рассмотрение варианта установки системы обнаружения вторжений-IPS
- Подключение модуля testcookie
- Использование tcdump – универсальное средство обнаружения уязвимостей
- Организация фильтрации трафика nginx

Методы борьбы

В качестве профилактических мер было принято решение предупредить персонал о возможных случаях, просьба внимательно проводить анализ текста и возможных ссылок на наличие ошибок, некорректном написании доменных имен, внесение персональных данных или данных компании только при согласовании со специалистом.

Case 2. Кража онлайн-курсов

Одним из ценностных предложений предлагаемых нашей компанией являются платные онлайн-курсы с баскетбольной тематикой. Компания столкнулась с проблемой воровства этих курсов. Злоумышленник, используя программу записи экрана, скопировал данные материалы с нашего сайта и опубликовал курсы в открытом доступе на видеохостинге YouTube. Количество платных подписчиков снизилось, так как в сообществе быстро распространилась информация о том, что курсы можно смотреть бесплатно – пользователи делились между собой ссылками на опубликованные вне платформы курсы.

Методы борьбы

Для решения возникшей проблемы мы решили предпринять следующие действия. Сначала, мы обратились в поддержку видеохостинга YouTube с просьбой удалить незаконно размещенные там видео курсы. Ее представители согласились помочь и заблокировали канал, на котором были опубликованы наши видеоматериалы. Также, было решено изменить пользовательское соглашение, в обновленной редакции которого содержалась бы информация о запрете нелегального копирования и распространения контента, а также информация о привлечение нарушителей к уголовной ответственности за нарушение авторских прав. Помимо этого, было мы приняли решение о добавлении вотермарки на все наши видеоматериалы. Она будет содержать индивидуальный номер пользователя, просматривающего контент для того, чтобы в случае его незаконного распространения было возможно вычислить злоумышленника и привлечь его к ответственности. Данные меры, по нашему мнению, должны сократить число случаев воровства наших видеокурсов и остановить отток платных подписчиков.