УЯЗВИМОСТИ ОНЛАЙНОВЫХ ИГР И СЕРВИСОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тетерин С. В.

Пачинин В. И. – канд. техн. наук, доцент

В современных онлайновых играх (World of Tanks и др.) существует уязвимость в части несанкционированного доступа, под которым понимается завладение доступом к учётной записи игрока лицом, не являющимся её владельцем, а под уязвимостью – возможность такого доступа.

Кроме чисто практических возможностей (электронная почта, поиск информации, общение в социальных сетях и др.), необходимых каждому пользователю компьютера или другого устройства, имеющего доступ к глобальной компьютерной сети, Интернет предоставляет своим фанатам также и развлекательные возможности в виде онлайновых игр и сервисов. Аудитории компьютерных игроков насчитывают десятки миллионов человек (например, World of Tanks – ~60 млн.). Всемирный интерес к World of Tanks понятен: игра является масштабным многопользовательским экшеном в реальном времени с динамичными танковыми PvP-сражениями, участие в которых требует от игрока умения планировать свои действия и слаженно работать в команде. В игре представлено более 150 моделей советских, немецких и американских танков. Глобальная карта игры обеспечивает массу потрясающих возможностей для любителей жёсткого кланового геймплея. Увлекательное, захватывающее дух сочетание экшена и грандиозных танковых баталий включает все элементы настоящего блокбастера. Великолепная графика позволяет игрокам в полной мере насладиться стремительными схватками на полях сражений.

Однако участвуя в игре, игроки используют свою личную информацию [1] (страна проживания, номер мобильного телефона, адрес электронной почты и др.) для формирования своей учётной записи в игре, а также совершения платежей и других операций, передавая ее сервисам онлайн-игр. Помимо этой информации, огромной ценностью являются игровые аккаунты (связки логина/пароля) и виртуальные предметы, которые продаются в интернете за большие деньги и представляют большую ценность для их обладателей.

В докладе рассматривается основная уязвимость онлайновых игр и сервисов – уязвимость в части несанкционированного доступа. При этом под несанкционированным доступом понимается завладение доступом к учётной записи игрока лицом, не являющимся её владельцем, а под уязвимостью (*vulnerability*) – недостаток в игре, используя который атакующий «обманывает» приложение — заставляет его совершить действие, на которое у него нет прав.

В этих условиях игровым компаниям, осуществляющим разработку онлайн-игр необходимы комплексные меры для защиты информации. Каждая онлайновая игра имеет определенный набор сервисов - спутников, таких как: платежные системы, позволяющие проводить онлайновые платежи; форумы для общения игроков; сайты поддержки пользователей, используемые для обработки запросов пользователей; комьюнити-сайты, предоставляющие новости, поиск игроков/гильдий и другую функциональность для расширения игровой вселенной в рамках проекта.

Типичная онлайновая игра разделена на две большие составляющие – серверная часть и игровой клиент, устанавливаемый на компьютеры пользователей. В отличие от серверной части, взлом которой является редкой и крайне не тривиальной задачей, клиент, поставляемый игрокам – уязвимое место для взлома. Обычно подобные взломы производятся с целью создания ботов – автоматизированных программ, способных моделировать поведение в игре живого человека. Боты используются для автоматической «прокачки» аккаунтов, что наносит вред самой игре и ее экосистеме.

Сервисы-спутники подвержены хакерским атакам на различных уровнях. Поскольку эти сервисы являются веб-приложениями, для них характерно большое количество уязвимых мест. Обычно цель хакера в таких случаях заключается в получении несанкционированного доступа к аккаунтам других людей.

Часто в архитектуру онлайновых игр и сопутствующих сервисов закладывается идея «единого аккаунта», который является удобным для пользователя и, одновременно, злоумышленника: игрок создает одну пару логин/пароль, и при помощи ее получается возможность доступа не только к своему аккаунту, но и к форуму, сайту поддержки, комьюнити-сайту и др. Таким образом, украв аккаунт из базы данных, например форума, злоумышленник получает доступ и к игровому аккаунту.

Для обеспечения защиты аккаунтов в докладе предлагаются следующие меры:

- секретные вопросы и подтверждение операций по телефону («привязка телефона»);
- установка «Captcha» на всех формах логина;
- установка защиты от подбора пароля (невозможность слишком частых попыток ввода пары логин/пароль); постоянное обновление и доработка форумов (обычно берутся стандартные форумы от стороннего производителя, которые нередко бывают полны уязвимостей).

Список использованных источников:

1. Тетерин С.В., Пачинин В.И. Информационная безопасность онлайновых игр и сервисов // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., 15–16 окт. 2013 года, Минск, Респ. Беларусь / редкол.: А. О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – 322 с. – С. 230-231.

Библиотека БГУИР