УДК 004.42

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОНЛАЙНОВЫХ ИГРАХ И СЕРВИСАХ

С.В. ТЕТЕРИН[1], В.И. ПАЧИНИН[2]

[1]СООО Гейм-Стрим
пр-т Партизанский, 178/2, офис 38, г. Минск, 220028, Республика Беларусь
hypnotypes@gmail.com

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
pachinin@bsuir.by

Анализируется основная угроза информационной безопасности в онлайновых играх и сервисах – угроза несанкционированного доступа к аккаунтам игроков и виртуальным предметам. Предлагается комплекс организационных и технических мероприятий по парированию этой угрозы.

Ключевые слова: онлайновая игра, защита информации, учётная запись, аккаунт, несанкционированный доступ.

Десятки миллионов людей проводят время в онлайновых играх. Для примера, аудитория World of Warcraft – ~11.4 млн человек, World of Tanks – ~60 млн, Guild Wars 2 – ~9 млн, Star Wars: The Old Republic – ~1.3 млн [1, 2]. Игроки используют свою личную информацию (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 и виртуальные предметы, которые продаются в интернете за большие деньги и представляют большую ценность для их обладателей.

В докладе рассматривается основная угроза информационной безопасности в онлайновых играх и сервисах – угроза несанкционированного доступа. При этом под несанкционированным доступом понимается завладение доступом к учётной записи игрока лицом, не являющимся её владельцем, а под аккаунтом – связка логина/пароля.

Самый несложный и практически не имеющий вариантов защиты способ кражи аккаунтов у пользователей – получение аккаунта из рук жертвы путем «социальной инженерии» – злоумышленник через социальные сети или простое общение с жертвой узнает некоторые данные от пользователя, такие как адрес e-mail, дату рождения, некоторые персональные данные (они могут быть использованы в качестве ответа на секретный вопрос при попытке восстановить доступ к аккаунту) и использует эти данные для получения аккаунта. Также популярным способом является «фишинг» – на почту пользователя приходит письмо, оформленное как письмо от компании-разработчика, с просьбой предоставить пароль от своего аккаунта. Разумеется, письмо подделано злоумышленником. Несмотря на некоторую наивность, данный способ часто приводит к положительным для хакера результатам. Довольно частый способ получения чужих аккаунтов – программы-кейлоггеры, записывающие символы, введенные с клавиатуры пользователя. Более изощренные хакеры могут использовать различные «эксплоиты» (бреши в системе), позволяющие, например, отобразить в браузере пользователя формы для ввода пароля и логина. Естественно, данные формы отправляют данные злоумышленнику. Так же возможны банальные «брутфорсы» (подборы паролей) по уже извест-

ным e-mail адресам. Это лишь некоторые из известных способов получения чужих аккаунтов.

В связи с вышесказанным, 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 аккаунт.

Для парирования вышеперечисленной угрозы (обеспечения защиты аккаунтов) в докладе предлагаются следующие меры:

– секретные вопросы при попытке восстановить доступ к аккаунту;

– подтверждения 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).

На стороне клиента для предотвращения взлома игры и создания ботов предлагается:

– все логические расчеты производить только на стороне сервера;

– формы ввода логина/пароля защищать Capthca;

– проводить надежную архивацию ресурсов игры;

– внедрять систему жалоб и доносов – игроки, которые заподозрят других игроков в «ботоводстве», должны иметь возможность быстро и удобно сообщить об этом администрации проекта; анти-чит системы на сервере.

Необходимо также проводить социальные работы с аудиторией игроков – периодически повышать их грамотность в области сетевой безопасности, напоминать игрокам простые правила: пароль должен быть сложным, администрация проекта никогда не запросит данные об аккаунте у самого пользователя, личные данные лучше не доверять непроверенным людям, антивирус должен быть всегда обновлен и запущен.