ИНФОРМАТИКА И ТЕХНИЧЕСКИЕ НАУКИ

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

УДК 621.3.29

М. Блащак[1], П. П. Урбанович[2]
[1]Люблинский католический университет Иоанна Павла II (Польша)
[2]Белорусский государственный технологический университет

АТАКИ НА МНОГОПОЛЬЗОВАТЕЛЬСКИЕ КОМПЬЮТЕРНЫЕ ИГРЫ И НЕКОТОРЫЕ МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Приведен анализ некоторых уязвимостей многопользовательских компьютерных игр и атак на сервер такой игры (на примере игры «Project I.G.I. 2: Covert Strike»). Часто в основе взаимодействия поставщиков и пользователей рассматриваемой услуги лежит модель free-to-play. Каждому участнику игры нужно соперничать с другими виртуальными игроками. Одна из самых распространенных целей атак злоумышленников – кража паролей и других учетных данных, необходимых для доступа к аккаунту игроков. В статье проанализированы механизмы и программные особенности реализации некоторых видов атак, основанных на ошибках в кодах программных платформ («движков») игр. Анализ сетевого трафика между сервером и клиентским приложением показал, что большинство атак можно блокировать, перехватывая и анализируя сетевой трафик. Одной из лучших систем для обеспечения безопасности сервера считается Linux, поскольку он имеет очень высокоэффективный брандмауэр, функционал которого является ключевым аспектом в решении проблемы нейтрализации атак на серверы многопользовательских компьютерных игр. В статье также описано авторское приложение, предназначенное для нейтрализации некоторых атак на сервер анализируемой игры.

Ключевые слова: многопользовательская компьютерная игра, атака, переполнение буфера, безопасность, программная платформа, сервер, клиент.

M. Błaszczak[1], P. P. Urbanovich[2]
[1]The John Paul II Catholic University of Lublin (Poland)
[2]Belarusian State Technological University

ATTACKS ON MULTIPLAYER COMPUTER GAMES AND SOME METHODS OF PROTECTION AGAINST THEM

The analysis of some vulnerabilities of multiplayer computer games and attacks on the server of such a game is given (on example the game “Project I.G.I. 2: Covert Strike”). Often the free-to-play model is the basis of interaction between suppliers and users of the analyzed service. Each participant in the game needs to rival not only with other virtual players. One of the most common targets of attackers is theft of passwords and other credentials necessary to access the player’s accounts. The article analyzes the mechanisms and software features of the implementation of some types of attacks based on errors in the codes of software platforms (“engines”) of the games. An analysis of network traffic between the server and the client application showed that most attacks can be blocked by intercepting and analyzing network traffic. One of the best systems for providing of server security is Linux, because it has a very high-performance firewall, the functionality of which is a key aspect in solving the problem of neutralizing attacks on multiplayer computer game servers. The article also describes an authoring software application intended for neutralization of some attacks on the server of the analyzed game.

Key words: multiplayer computer game, attack, buffer overflow, security, software platform, server, client.

Введение. Современные компьютерные игры (КИ) – огромная индустрия с денежным оборотом, сопоставимым с нефтяным бизнесом. Особой популярностью пользуются мультиплеерные (многопользовательские) игры (МПИ, англ. Mass Multiplayer Online Game, MMOG) [1]. МПИ – сетевая компьютерная игра, в которой большое количество игроков взаимодействуют друг с другом в виртуальном мире. Указанная популярность во многом связана с тем, что в основе взаимодействия пользователей лежит модель free-to-play – игра доступна бесплатно, а прибыль идет от продажи игровых предметов, ускоряющих получение опыта, и различной декоративной экипировки.

В индустрии КИ появились разнообразные способы монетизации. Разработчики МПИ создают виртуальные пространства, функционирующие на основе собственной экономической системы. Деньги этой системы привлекают не только инвесторов, но и злоумышленников. Число вредоносных программ, «ворующих» игровые предметы и «угоняющих» аккаунты пользователей, растет быстрыми темпами. Особенно уязвимы мобильные приложения, так как многие из них требуют ввода игроком данных банковской карты [2]. Любая отрасль, которая оперирует персональными данными, как правило, становится объектом атак со стороны тех, кто хочет получить эти данные. Игровая индустрия – не исключение.

Типичная онлайновая игра разделена на серверную часть и игровой клиент, устанавливаемый на компьютерах или мобильных устройствах игроков (пользователей).

Программная платформа КИ обеспечивает техническую базу, на основе которой реализуются такие функции, как рендеринг графики, имитация физических процессов, искусственный интеллект, управляющий поведением игровых персонажей, сеть, управление памятью и т. д. Учитывая очень высокую сложность этих программных платформ, невозможно ожидать отсутствия в них багов. И они действительно есть всегда. Эти недостатки сказываются на работе самих игр, а не аппаратных платформ, на которых они реализованы и функционируют, – локальных компьютерах, серверах или мобильных устройствах.

В [3] кратко проанализированы некоторые уязвимости сервера игры «Project I.G.I. 2: Covert Strike» [4].

В настоящей статье будут рассмотрены более подробно особенности некоторых атак на сервер МПИ (на примере игры [4]), а также меры по обеспечению его безопасности.

Основная часть. Существует много типов атак с использованием ошибок в программных кодах игр [5]. Одна из таких атак – «Format string attack» [6] – заключается в неправильной передаче параметров в функцию *printf*.

Атака на основе форматирования последовательности знаков. Атакующий обычно использует директиву *%n*, которая записывает количество символов, сохраненных данной функцией под область памяти, указанную в следующем аргументе, как в примере на рис. 1.

```
0000   2f 25 6e 25 6e 25 6e                                  /%n%n%n
```

Рис. 1. Пакет, используемый в атаке, форматирующей строки

Эту атаку очень легко осуществить. Самый простой способ – ввести комбинации символов *%n%n* в игровом чате. Это закрывает приложение на сервере. Не только чат подвержен такой ошибке.

Ввод указанной комбинации символов в любом месте приводит к той же реакции приложения. Приведенная строка кода воспринимается как команда сервера. Эта комбинация символов также может быть отправлена в пакете, содержащем имя игрока. На рис. 2 приведен фрагмент такого пакета.

```
0080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0   00 00 00 00 00 00 00 00 00 00 00 00 25 6e 25 6e   ............%n%n
00b0   25 6e 25 6e 25 6e 00 6c 6d 6e 6f 70 71 72 73 74   %n%n%n.lmnopqrst
00c0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Рис. 2. Атакующая строка в пакете с именем игрока

Другое место, где можно использовать атаку, – это чат игры. В качестве содержимого сообщения отправляется указанная строка. На рис. 3 показан фрагмент такого пакета.

```
0000   de ad be ef 0c 00 00 00 00 00 00 47 5a 01 18   ...........GZ..
0010   03 ab ab ab 01 00 00 00 ff ff ff ff 54 41 48 43   ............TAHC
0020   4c a4 00 00 4a 6f 6e 65 73 3a 20 25 6e 25 6e 0a   L...Jones: %n%n.
0030   00 5f 00 00 00 00 80 3f 00 00 00 00 00 00 00 00   ._.....?........
0040   00 00 00 00 00 00 80 3f 00 00 00 00 00 00 00 00   .......?........
```

Рис. 3. Фрагмент пакета с сообщением, содержащим атакующую строку

Для этого типа атаки была создана защита в виде патчей. Однако такая защита приводит к возможности реализации иных видов атак, не менее опасных. Например, проблема смены так называемой игровой карты. Если карта на сервере поменялась, игроки могут встретить трудности с идентификацией.

Атака с переполнением буфера имени игрока. В области информационной безопасности

корпоративных ресурсов очень остро стоит проблема атак на сеть путем переполнения буфера [6]. Основная особенность такой атаки состоит в следующем: если атакующий сможет «подсунуть» компьютеру некоторые инструкции в виде кода, компьютер выполнит эти инструкции. Это является основой для нападения, связанного с переполнением буфера. С формальной стороны переполнение буфера возникает, когда компьютерная программа записывает данные («подсунутые» инструкции) за пределами пространства, выделенного в памяти буфера.

Это приводит к перезаписи других данных в памяти, которые могут потребоваться для правильного функционирования приложения. Одним из способов использования этой атаки является переполнение буфера для имени игрока. Приложение имеет ограничение имени в 19 символов. Можно войти в игру, введя соответствующие параметры в командной строке. Если вводится строка символов длиной больше 64 в параметре *name*, игрок войдет в систему с именем лишь из 64 символов. Чтобы воспользоваться ошибкой переполнения буфера, нужно подготовить сетевые пакеты, отвечающие за присоединение к игре. Для этого следует отправить пакет с именем, например, длиной 66 символов (рис. 4).

Рис. 4. Фрагмент пакета переполнения буфера имени игрока

Довольно хорошо с подобной проблемой можно справиться, используя межсетевые экраны для анализа сетевого трафика [7].

Атака с переполнением буфера ключа. Это атака, аналогичная предыдущей, но здесь используется ключ к игре. При вступлении в игру каждый игрок отправляет свой ключ (CD-KEY) в пакете, который верифицируется. Пример пакета показан на рис. 5.

Содержимое пакета включает в себя зашифрованный ключ игрока. Это содержимое можно разделить на две части. Первая, отмеченная подчеркиванием, никогда не меняется. Ее размер составляет 32 байта. Остальная часть изменяется в каждом отправленном пакете.

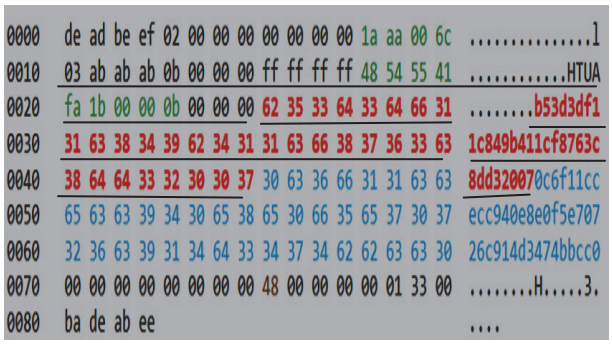

Рис. 5. Пример пакета авторизации с уникальным CD-ключом

Если отсылается пакет с более длинным ключом на сервер, серверное приложение перестанет работать. Защита сервера от переполнения буфера имени игрока также является защитой от атаки с переполнением буфера ключа, поскольку этому пакету предшествует подключение к игре.

Атака по запросу о ключе. Механизм проверки CD-ключа имеет и иное слабое место. Чтобы проверить, используется ли иными игроками ключ, представленный данным игроком, приложение использует онлайн-валидацию. Ключ отправляется на серверы *Gamespy*, и затем отправитель получает ответ о результатах валидации. Все сообщения шифруются с помощью функции XOR, используя для шифрования строку *gamespy*. В указанном ответе встречаются запросы, разделенные символом *backslash*. При чтении запросов появляется ошибка. Если игрок отправит на сервер сообщение с одним символом *backslash*, приложение закроется. Проблема здесь кроется в плохо запрограммированном анализаторе запросов. Это можно проиллюстрировать следующим фрагментом кода:

```
int size = strchr(buff + 1, '\\') - buff;
  if(size > 32) return;
  strncpy(querybuff, buff + 1, size);
```

Переменная *buff* содержит запрос. В нем отыскивается знак «\». Затем проверяется условие, и извлеченный текст помещается в переменную *querybuff*. Заметна ошибка в этом программном коде. Значение, возвращаемое функцией *strchr*, не проверяется, поэтому, если функция не находит косую черту и возвращает «0», функция *strncpy* выдаст исключение, потому что значение переменной *size* будет отрицательным.

Решением описанной проблемы является патч, выпущенный Luigi Auriemm. Тип *signed* изменен на *unsigned*, поэтому значение не может быть отрицательным [8].

Атака на основе модификации карты. О карте мы вспоминали в анализе атаки на основе форматирования последовательности знаков.

Редактор карт доступен каждому. Некоторые модификации могут закрыть программу. Файлы карты на сервере должны совпадать с файлами карты у игрока. Карта содержит различные объекты: здание, стена, лестница и др. Каждый объект имеет свой идентификационный номер. Это важно для интерактивных объектов, таких как двери, кнопки, лестницы. Когда игрок использует один из объектов, он отправляет на сервер пакет с идентификационным номером объекта. Затем сервер отсылает пакеты с информацией о деятельности игрока другим участникам игры. Благодаря этому каждый может увидеть эффект от использования объекта, например открытие двери. Проблема возникает, когда игрок (или злоумышленник) использует объект с идентификационным номером, которого сервер «не знает». В этом случае программа закрывается.

Карта может состоять из ограниченного количества объектов. В анализируемой игре можно создать максимум 4096 объектов. Это облегчает защиту от этой атаки.

Если у всех будет одинаковый файл, который использует максимальное количество объектов, игра не закроется. Другой способ – создать базу данных всех используемых идентификационных номеров объектов и проверять, содержит ли пакет идентификатор из этой базы данных.

Кроме рассмотренных, существуют и иные виды атак на серверные и клиентские приложения данной и других компьютерных игр. Часто решением возникающих проблем занимаются не только разработчики игр, но и сами игроки. В последнем случае появляются специализированные программные средства.

Специализированные программные средства для защиты сервера игры. В доступных источниках содержится мало информации о программных продуктах, предназначенных для решения указанных задач.

Вероятно, одним из первых было многооконное приложение Project1. Оно имеет много функций, облегчающих работу администратора (например, отправка команд на сервер, написание общих сообщений игрокам, механизмы предупреждения обмана игроков). Project1 предоставляет много важной информации о сервере: количество игроков, текущая карта, время игры, список игроков каждой команды, статистика игроков, IP-адреса, разговоры в чате.

Приложение Mautorun основано на анализе сетевых пакетов. Приобрело большую популярность среди администраторов серверов.

Одной из программ, предотвращающих атаки на сервер, является AutoBan. Его основная функция заключается в обнаружении атак с переполнением буфера. Это обнаружение основано на анализе разницы во времени, соответствующего отправлению пакетов присоединения к игре. Как правило, атакующая сторона отправляет пакеты в течение 1 с. Пример соответствующих линеек кода (в действительности – двух) выглядит так:

```
[13:20:01] Server info sent to
192.168.1.1:26014
[13:20:01] NETWORKPACKET_TYPE_
CLIENTCONNECT [192.168.1.1:26015]
```

Можно заметить, что обе строки были созданы на протяжении 1 с. Это означает, что были отправлены вредоносные пакеты. Программа AutoBan извлекает IP-адрес и блокирует его. Если сервер работает быстро, последний пакет, который должен закрыть сервер, будет нейтрализован.

Второй способ обнаружить атаку – это проверить порты. Если хакер отправляет каждый пакет из другого сокета, то это приводит к изменению порта. Если две линии указывают на разные порты, это – вероятно, атака.

Авторское приложение для защиты сервера МПИ. Для нейтрализации описанных выше атак на сервер анализируемой игры нами разработано специальное приложение.

Вся система состоит из трех модулей (рис. 6).

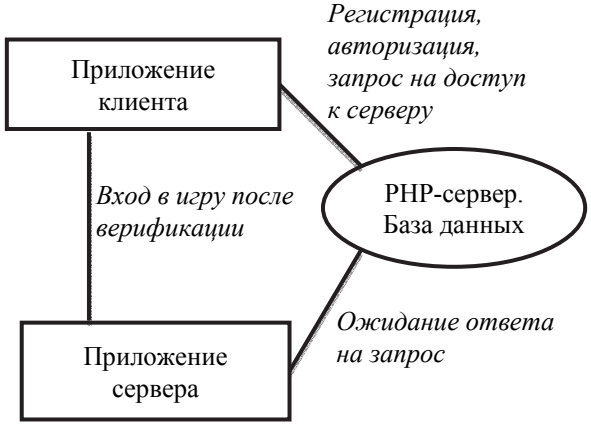

Рис. 6. Общая схема взаимодействия модулей системы

Клиентская программа используется для взаимодействия с пользователем, отвечает за регистрацию и вход в систему, настройку учетной записи и присоединение к игре. Второй модуль – это PHP-сервер с базой данных на платформе MySQL. Его задача – проанализиро-

вать данные, полученные из клиентской программы, проверить их корректность и возвратить необходимую информацию игроку. Информация о пользователях хранится в базе данных. Последний модуль представляет собой серверное приложение, которое было интегрировано в существующую программу управления сервером. Модуль предназначен для проверки того, запрашивает ли пользователь доступ к серверу, а также для контроля исключений в брандмауэре. Добавляя исключения в брандмауэр, пользователь получает доступ к серверу. На рис. 7 представлен алгоритм регистрации пользователя.

Клиентская часть написана на C# с использованием технологии .NET. Основным преимуществом этой технологии является доступ ко многим библиотекам, содержащим готовые решения анализируемой проблемы.

Серверное приложение создано на Java с использованием технологии Maven и библиотеки *jnetpcap*, предназначенной для анализа сетевого трафика. Коммуникационный сервер создан с помощью технологии управления базами данных MySQL и языка PHP.

К особенностям разработанного приложения можно отнести следующее.

После получения списка ожидающих пользователей программа вызывает команду для добавления инструкции в брандмауэр сервера:

```
iptables -A INPUT -s 192.168.0.1 -p udp -
-dport 26001 -j ACCEPT
```

Такое правило принимает UDP-пакеты, поступающие на порт 26001 с IP-адреса 192.168.0.1.

Уникальный ключ CD-KEY должен быть сохранен в системном реестре.

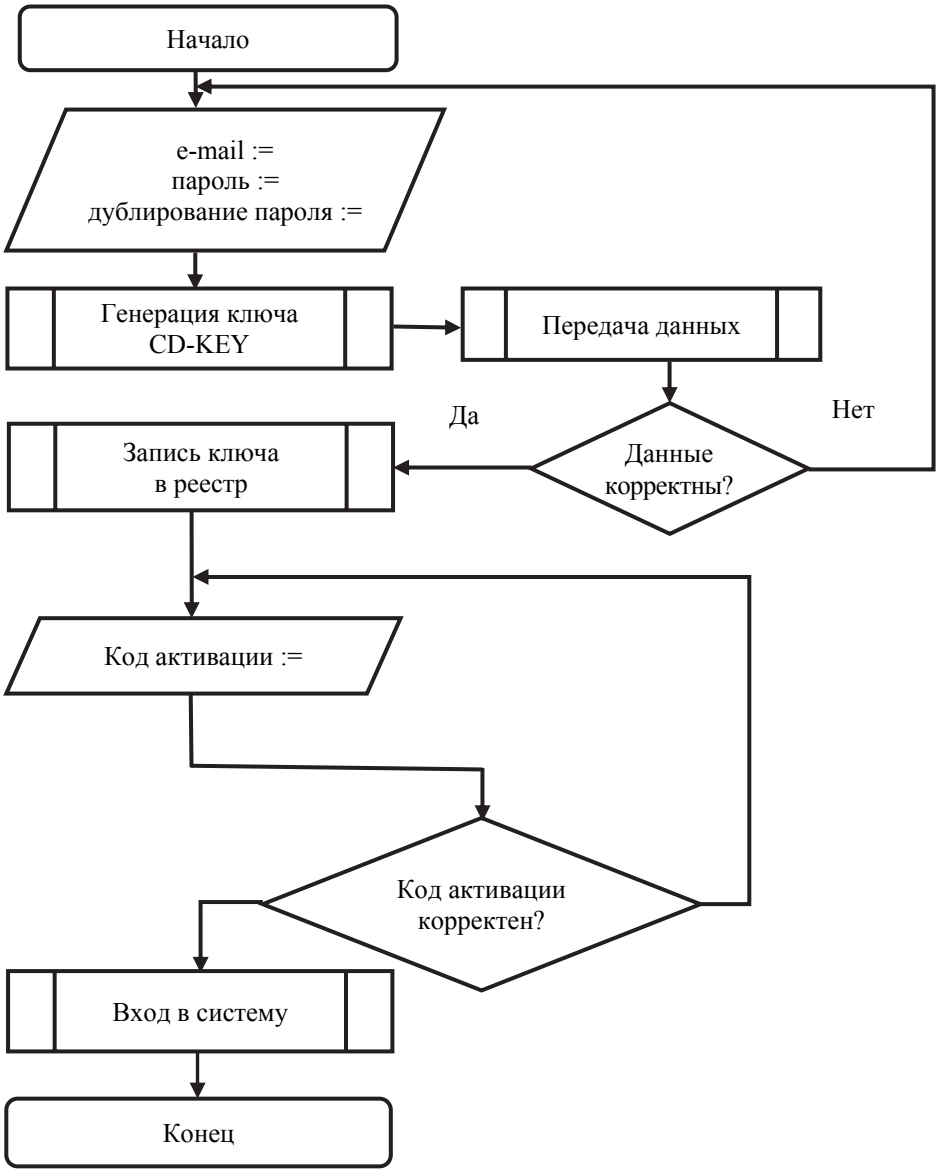

Рис. 7. Алгоритм регистрации пользователя для авторского приложения

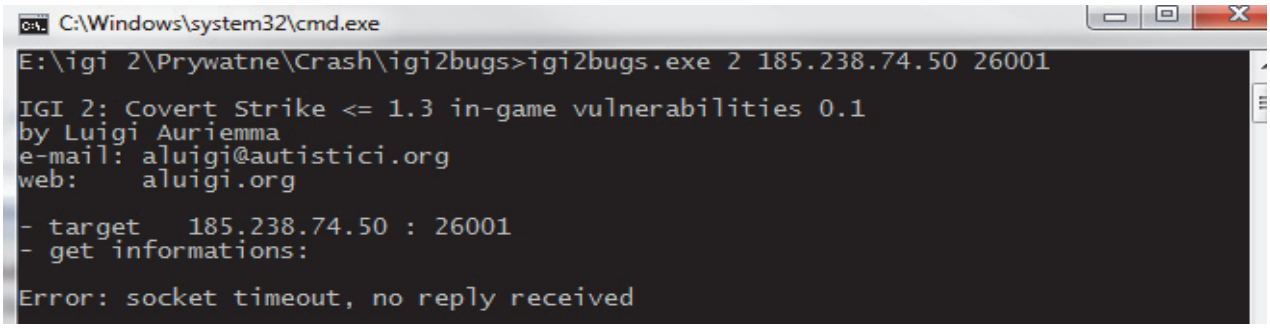

Рис. 8. Иллюстрация реализации атаки без регистрации пользователя

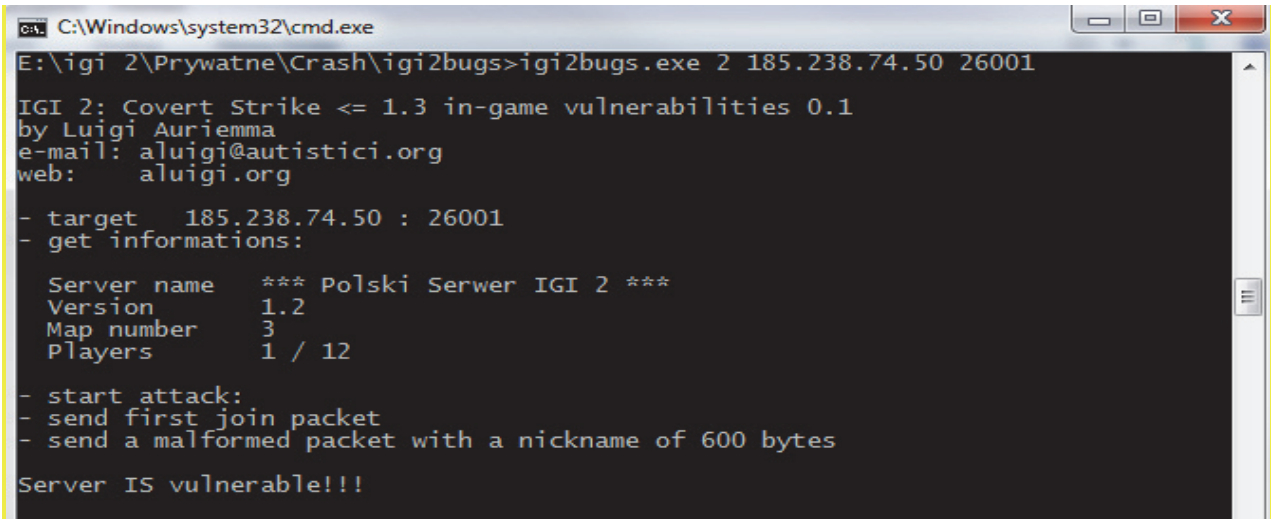

Рис. 9. Иллюстрация реализации атаки зарегистрированного пользователя

Программа на сервере проверяет статус игроков каждые 5 с, отправляя запрос в базу данных. Доступ к серверу получается путем добавления необходимой инструкции в брандмауэр. Если попытаться получить доступ к серверу без запроса доступа, то соответствующие пакеты будут проигнорированы, потому что весь входящий трафик будет заблокирован. Попытка войти на сервер без использования клиентской программы не приведет к получению ответа от сервера.

Попытка атаковать сервер с помощью хорошо известной программы *igi2bugs* также потерпит неудачу, как это показано на скриншоте (рис. 8), поскольку сервер отклоняет весь трафик. Это делает систему невосприимчивой к атакам незарегистрированных пользователей.

Если пользователь зарегистрируется, он все равно не сможет атаковать, поскольку он не отправил запрос на доступ к серверу. Только после нажатия кнопки «Присоединиться к игре» («Join game») клиентская программа отправляет такой запрос. К сожалению, система не в состоянии заблокировать попытку атаки зарегистрированного игрока. Такую ситуацию иллюстрирует рис. 9.

В большинстве компьютерных игр последнего поколения практически нет уязвимостей, свойственных описанной игре. Но нет ни одного приложения, абсолютно защищенного перед атаками. Невозможно также защитить многопользовательскую компьютерную игру на 100%. Однако можно снизить ее уязвимости на основе анализа предыдущих событий.

Заключение. Анализ сетевого трафика между сервером и клиентским приложением (игроком) показал, что большинство атак на сервер многопользовательской компьютерной игры можно заблокировать.

При выборе системы, на которой будет запускаться игровой сервер, необходимо учитывать время отклика при добавлении необходимых инструкций в брандмауэр. Система Linux позволяет фильтровать сетевой трафик, используя *iptables* [8]. Брандмауэр Windows медленнее реагирует на добавление новых инструкций. Также доступны улучшенные серверные приложения, которые блокируют некоторые виды атак.

Наш практический опыт показал достаточно высокую эффективность использования масштабирования базовой программной платформы компьютерной игры «Project I.G.I. 2: Covert Strike» для защиты игрового сервера от злоумышленников.

Литература

1. Ciesielka P., Urbanovich P. P. Security of applications for computer games [Электронный ресурс] // Информационные технологии: материалы 83-й науч.-техн. конф. проф.-препод. состава, науч. сотр. и аспирантов, Минск, 4–15 февр. 2019 г. / Белорус. гос. технол. ун-т. Минск, 2019. С. 26–28. URL: https://www.belstu.by/Portals/0/userfiles/37/09-tezisi-PPS-IT-2019_2.pdf (дата обращения: 20.09.2019).

2. Видеоигры и информационная безопасность: как не проиграть [Электронный ресурс]: [сайт]. [2019]. URL: https://www.securitylab.ru/blog/company/falcongaze/338191.php (дата обращения: 20.09.2019).

3. Błaszczak M., Urbanovich P. P. Server security of the multiplayer game «PROJECT I.G.I. 2: COVERT STRIKE» [Электронный ресурс] // Информационные технологии: материалы 83-й науч.-техн. конф. проф.-препод. состава, науч. сотр. и аспирантов, Минск, 4–15 февр. 2019 г. / Белорус. гос. технол. ун-т. Минск, 2019. С. 117–119. URL: https://www.belstu.by/Portals/0/userfiles/37/09-tezisi-PPS-IT-2019_2.pdf (дата обращения: 20.09.2019).

4. Логинов А. Краткие обзоры. IGI 2: Covert Strike [Электронный ресурс]: [сайт]. [2019]. URL: https://www.igromania.ru/article/7721/Kratkie_obzory_IGI_2_Covert_Strike.html (дата обращения: 21.04.2019).

5. Урбанович П. П. Защита информации методами криптографии, стеганографии и обфускации. Минск: БГТУ, 2016. 220 с.

6. Howard M., LeBlanc D. Writing Secure Code, Redmond. Washington: Microsoft Press, 2003. 768 p.

7. Урбанович П. П., Романенко Д. М., Кабак Е. В. Компьютерные сети. Минск: БГТУ, 2011. 400 с.

8. Luigi Auriemma. Gamespy SDK used for online cd-keys validation in third party code [Электронный ресурс]: [сайт]. [2019]. URL: http://aluigi.altervista.org/adv/gshboom-adv.txt (дата обращения: 30.09.2019).

References

1. Ciesielka P., Urbanovich P. P. [Security of applications for computer games]. *Informatsionnyye tekhnologii*, Minsk, 2019, pp. 26–28 (In Russian). Available at: https://www.belstu.by/Portals/0/userfiles/37/09-tezisi-PPS-IT-2019_2.pdf (accessed 20.09.2019).

2. *Videoigry i informatsionnaya bezopasnost'*: *kak ne proigrat'* [Video games and information security: how not to lose]. Available at: https://www.securitylab.ru/blog/company/falcongaze/338191.php (accessed 20.09.2019).

3. Błaszczak M., Urbanovich P. P. [Server security of the multiplayer game "PROJECT I.G.I. 2: COVERT STRIKE"]. *Informatsionnyye tekhnologii*, Minsk, 2019, pp. 26–28 (In Russian). Available at: https://www.belstu.by/Portals/0/userfiles/37/09-tezisi-PPS-IT-2019_2.pdf (accessed 20.09.2019).

4. Loginov A. *Kratkiye obzory. IGI 2: Covert Strike* [Brief reviews. IGI 2: Covert Strike]. Available at: https://www.igromania.ru/article/7721/Kratkie_obzory_IGI_2_Covert_Strike.html (accessed 21.04.2019).

5. Urbanovich P. P. *Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii* [Information protection using cryptography, steganography and obfuscation methods]. Minsk, BGTU Publ., 2016. 220 p.

6. Howard M., LeBlanc D. Writing Secure Code, Redmond. Washington, Microsoft Press, 2003. 768 p.

7. Urbanovich P. P., Romanenko D. M., Kabak E. V. *Komp'yuternyye seti* [Computer networks]. Minsk, BGTU Publ., 2011. 400 p.

8. Luigi Auriemma. Gamespy SDK used for online cd-keys validation in third party code. Available at: http://aluigi.altervista.org/adv/gshboom-adv.txt (accessed 30.09.2019).

Информация об авторах

Блащак Матэуш – магистрант. Люблинский католический университет Иоанна Павла II (20-950, г. Люблин, Аллеи Рацлавицке, 14, Польша). E-mail: mateuszblaszczakb@gmail.com

Урбанович Павел Павлович – доктор технических наук, профессор, профессор кафедры информационных систем и технологий. Белорусский государственный технологический университет (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: p.urbanovich@belstu.by, uppkul@kul.lublin.pl

Information about the authors

Błaszczak Mateusz – Master's degree student. The John Paul II Catholic University of Lublin (14, Aleje Racławickie, 20-950, Lublin, Poland). E-mail: mateuszblaszczakb@gmail.com

Urbanovich Pavel Pavlovich – DSc (Engineering), Professor, Professor, the Department of Information Systems and Technology. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: p.urbanovich@belstu.by, uppkul@kul.lublin.pl

Поступила после доработки 25.11.2019