УДК 303.7
Сєлетков Є. А.[1], Зайко Т. А.[2]
[1] студ. гр. КНТ-128сп НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

ІНФОРМАЦІЙНИЙ ЗАХИСТ В ІНДУСТРІЇ ВІДЕОІГОР

Ігрові сервіси – це основний спосіб отримання ігор та контенту. У домашніх консолях це сервіси від виробників пристрою, на зразок Xbox Store і PS Store, на персональних комп'ютерах є Steam, Epic Games Store, Origin, Uplay, GOG, Battle.net, а у випадку з мобільними пристроями - Google Play і App Store [1].

Найпопулярнішим на персональних комп'ютерах є сервіс компанії Valve Steam. Корпорація Valve є відомим у світі розробником відеоігор, а також спеціалізується на цифровій дистрибуції. Сервіс Steam надає послуги цифрової дистрибуції, багатокористувацьких ігор і спілкування гравців. Через Steam поширюється близько 23000 продуктів, кількість активних користувачів перевищує 125 мільйонів, щодня сервісом у середньому користуються 14 мільйонів осіб. По оцінці експертів сервіс Steam охоплює 70% ринку цифрової дистрибуції відеоігор у світі.

9 грудня 2018 р. компанія Valve обмежила обмін предметами в сервісі Steam для користувачів, які не використовують двоетапну перевірку через мобільний додаток. Щоб донести до геймерів важливість застосування цього методу, компанія привела тривожну статистику злому облікових записів і докладніше розповіла про причини свого рішення. З'ясувалося, що щомісяця в руки зловмисників потрапляють близько 77 тис. аккаунтів, і кількість зломів продовжує зростати.

Існує два варіанти викрадення інформації:

1) За допомогою програми, яка відсилає з Вашого комп'ютера інформацію зловмисникові. Говорячи простіше це вірус (шпигун, кейлогер, троян та інші).

2) Користувач добровільно передає інформацію.

Зазвичай таким способом є фішингові сайти. Це саме ті сайти, які мають ідентичний вигляд оригінального сайту, але з іншою адресою (доменом). Адреса буває дуже схожою на адресу необхідного вам сайту, але візуально його можна прийняти за справжній. Відмінність може бути в одній букві по типу: mn, nn, mm або nm від повної адреси [2].

Такі фішингові сайти могли прислати ваші недавно додані друзі або зловмисник який вкрав аккаунт вашого друга і пише під його виглядом. Частіше всього такі сайти присилають з проханням проголосувати або з наданням можливості отримати гру або внутрішньоігрові речі безкоштовно

або недорого.

Бувають більш продумані ходи з боку викрадача інформації.

Він може спочатку вистежувати Вашу мережеву активність завдяки можливостям Steam і подружитися під час гри, наприклад.

Далі почне вивчати Ваш список друзів і аналізувати активність спілкування.

Після цього, в один прекрасний момент, він повністю переробить свій профіль під профіль Вашого друга (будуть максимально схоже збігатися імена, аватарки і інша інформація про аккаунт) та піде з Вами на контакт [3].

Щоб захистити свій обліковий запис Steam доцільно використовувати Steam Guard. Steam Guard - це додатковий рівень безпеки, який може бути використаний на ваш обліковий запис Steam. Перший рівень безпеки - ваші облікові дані: логін аккаунта і пароль. Активована функція Steam Guard ускладнить доступ до аккаунту для сторонніх осіб. Якщо на акаунті активована функція Steam Guard, для входу в нього з неавторизованого пристрою буде потрібно спеціальний коддоступу. Залежно від ваших налаштувань Steam Guard, код доступу ви отримаєте або в повідомленні, надісланому на контактну адресу електронної пошти, або через мобільний додаток Steam [2].

Також є додатковий спосіб захисту Сімейний перегляд, який більше підходить для контролю дітей, але підійде також і для захисту. Для користування ним треба створити додаткову пошту та придумати 4-значний пароль. При вході в Steam буде доступна тільки бібліотека користувача з такою кількістю ігор яку він вказав при налаштуванні. Можна вказати як всі ігри так і ні одної, що буде краще для захисту. Щоб мати можливість користуватися треба вийти з Сімейного перегляду увівши придуманий пароль.

Популярність Steam стрімко зростає, а це значить, що будуть з’являтися нові способи обману користувачів. Не виключено, що це буде шкідливий код, який Ви по необережності знайдете на просторах Інтернету. Він же в свою чергу вчепитися в браузер і надалі буде переадресовувати на фішингові сторінки [3].

В більшості інших сервісах теж є додаткові захисні функції. Наприклад двоєтапна аутентифікація через пошту або через Google Authenticator як в Uplay.

Отже сьогодні інформаційний захист персональних даних в ігровій індустрії залишається відкритою. Навіть якщо користуватися всіма перерахованими вище методами захисту це на 100% не захистить аккаунт від злому та шахрайства. Тому потрібно бути дуже обережним реєструючись на різних сайтах через аккаунт Steam або аккаунти інших сервісів та ретельно перевіряти такі сайти на дійсність та чесність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Відеоігри та інформаційна безпека: як програти [Електронний ресурс]. – Режим доступу:
https://www.securitylab.ru/blog/company/falcongaze/338191.php (дата звернення – 05.03.2020). – Назва з екрана.
2. Безпека соціально-економічних процесів в кіберпросторі [Електронний ресурс]. – Режим доступу:
https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf (дата звернення - 05.03.2020). – Назва з екрана.
3. Як захистити свій Steam аккаунт [Електронний ресурс]. – Режим доступу: https://steamcommunity.com/sharedfiles/filedetails/?id=252672665 (дата звернення – 05.03.2020). – Назва з екрана.