АНАЛІЗ ЕФЕКТИВНОСТІ ПРОТИДІЇ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ КОМПАНІЙ HID-АТАКАМ

Гриньов Р.С., Шаповал З.В., Петренко О.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Питання безпеки в сучасних операційних системах не втрачає актуальності. Існує безліч різних векторів атак [1-3]. Деякі з них вже давно відомі, деякі тільки з'явилися. Безмежна довіра операційних систем до таких пристроїв, як клавіатура або маніпулятор "миша" може нести загрозу безпеці. Якщо зібрати пристрій, який буде емулювати необхідне введення даних, і під'єднати його до комп'ютера, можна завдати серйозної шкоди системі. Портативні носії даних дуже часто є джерелами поширення вірусного програмного забезпечення. Якщо раніше зловмисники використовували файл autorun.inf в корені флеш накопичувача, то останнім часом все частіше записують програму безпосередньо в мікроконтролер.

Сфери застосування такого запрограмованого мікроконтролера можуть бути різні, від застосування адміністраторами систем, фахівцями з безпеки під час проведення прихованого тесту на проникнення в компанії до використання такого пристрою зловмисниками. При підключенні подібного пристрою, ні система, ні, наприклад, антивірус не помічають вторгнення, оскільки визначають його як звичайну клавіатуру.

Метою доповіді є використання статистичних даних про кількість інцидентів за попередні роки для прогнозування кількості інцидентів на майбутні періоди за допомогою регресійного аналізу. На основі отриманих результатів можуть бути прийняті відповідні міри по реагуванню.

В доповіді наводяться результати проведеного аналізу статистичних даних та прогноз кількості можливих інцидетів. Наведені дані показують, що кількість атак в найближчий час суттєво зросте, тому є актуальною розробка та впровадження нових методів та засобів захисту.

Також в роботі представлені варіанти захисту від HID-атак.

Список літератури

1. The fighting HID emulator - URL: http://developers-club.com/posts/141838/.
2. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.
3. Evil USB the HID-emulator or it is simple Peensy- URL: http://developers-club.com/posts/141838/