МЕТОДИ ВИЯВЛЕННЯ ВІРУСІВ У ЗОБРАЖЕННЯХ ФОРМАТУ BMP ТА ПРОТИДІЇ HID-АТАКАМ

Гриньов Р. С., Сєвєрінов О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Питання безпеки в сучасних інформаційних системах є досить актуальним. Існує безліч різних векторів атак. Довіра операційних систем до таких пристроїв, як клавіатура або маніпулятор "миша" може нести загрозу безпеці через проведення HID-атак. У даному випадку вектор атаки лежить на стику технології і соціальної інженерії. А саме, вимагає від потенційного зловмисника можливості фізично підключити пристрій, який визначиться як пристрій введення і самостійно виконає необхідні для нього дії.

Однак сучасні засоби захисту не можуть виявити та протидіяти даній атаці, оскільки вважають HID-пристрої повністю довіреними.

Такі атаки стають ще більш небезпечними у поєднанні з методами, що дозволяють приховати вірус у зображеннях формату BMP. Це дозволяє обійти засоби захисту, що не витрачають ресурси на сканування звичайних зображень, оскільки вважають їх безпечними.

Метою доповіді є аналіз результатів впровадження програмного забезпечення, що реалізує методи виявлення вірусів у зображеннях формату BMP та протидію HID-атакам. Перша програма виявляє та протидіє HID-атакам на основі аналізу швидкості введення тексту та її змін. Програмне забезпечення функціонує як фоновий процес, дозволяє блокування клавіатури у випадку виявлення небезпеки та реєстрацію атак в журналі. Друге програмне забезпечення перевіряє зарезервовані поля зображення BMP на предмет наявності вірусів.

Проведені дослідження довели, що розроблені засоби захисту є більш ефективними в порівнянні зі звичайними засобами для протидії подібним атакам.

У сучасному інформаційному світі питання захисту даних і безпеки стоїть дуже гостро, особливо при створенні захищених систем. Необхідно враховувати різні аспекти та вектори атак. Особливо ті, які базуються на соціальної інженерії і вразливості операційних систем.

Список літератури

1. Гриньов Р.С., Сєвєрінов О.В. Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення // Комп'ютерні та інформаційні системи і технології. – 2019. – с. 75.

2. Гриньов Р., Сєвєрінов О. В. Аналіз ефективності протидії сучасних засобів захисту компаній HID-атакам. – 2019.

3. Гриньов Р.С., Сєвєрінов О.В. Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP // Радіотехніка. – 2019. – Т. 3. – №. 198. – С. 192-202.

4. Гриньов Р.С., Сєвєрінов О.В., Власов А.В. Метод виявлення та протидії вірусам у зображеннях формату BMP // Радіотехніка. – 2020. – Т. 1. – №. 200. – С. 195-200.