УДК 621.396:004.056

# АНАЛІЗ ВРАЗЛИВОСТЕЙ БЕЗПРОВІДНИХ КЛАВІАТУР

Черняк М.А.
Науковий керівник — ст. викладач Ликова Г.О
Харківський національний університет радіоелектроніки, каф. КріСТЗІ,
м. Харків, Україна
тел. +380660169405, email: maksym.cherniak@nure.ua

This work warns about the security risks of wireless keyboards and a hacking method called MouseJack. It highlights the importance for organizations to make sure that employees' wireless keyboards are secure and not vulnerable.

Із розвитком технологій та мобільності людей з’явилася потреба у використанні бездротових технологій, які із часом дісталися і до звичних для нас речей таких як бездротова клавіатура. Незважаючи на усі зручності, під час її використання є і свої ризики.

Одна з найпопулярніших вразливостей яка використовується проти бездротових клавіатур є MouseJack. MouseJack — це клас уразливостей, що впливає на переважну більшість бездротових, не Bluetooth-клавіатур та мишок. Ці периферійні пристрої підключаються до комп'ютера за допомогою радіопередавача, зазвичай це невеликий USB-радіоприймач. Оскільки з'єднання бездротове, а рухи миші та натискання клавіш передаються за допомогою радіохвиль, можна скомпрометувати комп'ютер жертви, передаючи спеціально створені радіосигнали за допомогою радіомодулю який підтримує потрібну частоту, зазвичай це 2,4 ГГц.

MouseJack здебільшого використовує три методи для компрометації бездротового USB-пристрою, який з'єднано з мишею або клавіатурою, і на який передається інформація щодо рухів миші або натискань клавіш які у подальшому можна буде використати для застосування вразливостей

Введення натискань клавіш у вигляді підробленої миші. У цьому випадку вразливий адаптер не використовує зашифроване з'єднання з мишею користувача, тому зловмисник може надсилати дані безпосередньо на адаптер під виглядом миші користувача. Крім того, адаптер не перевіряє чи миша надсилає лише дії які притаманні для миші, а саме її рух. Натомість він приймає дії клавіатури від підробленої миші та обробляє їх так, ніби вони надходять з клавіатури. Це дозволяє зловмиснику виконувати команди на комп'ютері, діючи як миша користувача;

Введення натискань клавіш у вигляді підробленої клавіатури. На відміну від мишей, клавіатури зазвичай використовують зашифроване з'єднання, що унеможливлює перехоплення даних з клавіатури. Однак вразливий адаптер все одно приймає незашифрований зв'язок з клавіатурою, що дозволяє зловмиснику її імітувати та виконувати команди на комп'ютері користувача;

Примусове підключення фейкової миші або клавіатури. Бездротові

клавіатури та миші дозволяють користувачам об'єднувати свої пристрої в пару у випадку, якщо один з них загубився і потребує заміни. Вразливий адаптер не обмежує належним чином сполучення пристроїв (яке зазвичай ініціюється користувачем за допомогою фізичної кнопки), і це дозволяє зловмиснику емулювати клавіатуру або мишу, надсилаючи команди на комп'ютер користувача.

Незважаючи на ці три основні вразливості бездротових клавіатур, є й інші, які спрямовані проти конкретних пристроїв, що схожі на вищезгадані, але мають певні унікальні особливості. Наприклад, коли використовується шифрування під час комунікації між клавіатурою та USB-радіоприймачем.

До них належать «CVE-2019-13054» та «CVE-2019-13055». Для їх експлуатації нам спочатку потрібен фізичний доступ до USB-радіоприймача. Із нього ми копіюємо дані ключа та у подальшому використовуємо для розшифрування пакетів даних які надходять від клавіатури або створювати власні.

Вразливості бездротових клавіатур показують, що навіть надійні на перший погляд пристрої, можуть бути вразливими до несподіваних недоліків безпеки. Організації де вони використовуються повинні провести належну перевірку, щоб переконатися, що бездротові периферійні пристрої, які вони видали співробітникам, не є вразливими до MouseJack та схожих до нього. У деяких випадках виробники випускають оновлення прошивки для вразливих пристроїв, які слід застосовувати там, де це доречно. У всіх інших випадках уражені пристрої слід викинути і замінити на невразливі (або дротові) альтернативи.

В роботі розглянуто додаткові методи підвищення безпеки при користуванні бездротовими пристроями вводу даних.

Список використаних джерел:

1. Use a wireless mouse? This $15 hack could compromise your laptop. [Електронний ресурс]: https://www.cnet.com/news/privacy/i-got-mousejacked/ Дата звернення: 11.03.2024

2. Wireless peripheral hijacking. [Електронний ресурс]: https://www.crowe.com/cybersecurity-watch/wireless-peripheral-hijacking-mousejack-attacks-explained-dgs Дата звернення: 11.03.2024

3. Logitech wireless USB dongles vulnerable to new hijacking flaws. [Електронний ресурс]: https://www.zdnet.com/article/logitech-wireless-usb-dongles-vulnerable-to-new-hijacking-flaws/ Дата звернення: 11.03.2024