УДК 681.324
А.Дьячук
(Національний технічний університет України “Київський політехнічний інститут”)

КОМП’ЮТЕРНІ ВІРУСИ ОСВОЮЮТЬ НОВІ ПРОСТОРИ

Наприкінці XX століття (1996-98 роки) Internet стає основним постачальником вірусів (у кінці 2003р. 61% комп’ютерних вірусів складали троянські програми, в 2005 р. – вже біля 70%, 2006–2007 р.р. – троянські програми та спам ще збільшили свою частку).

Як бачимо, проблема комп’ютерних вірусів не нова, і якщо спочатку вірусів можна було нарахувати близько десяти, то зараз їх декілька десятків тисяч, і розробники відпочивати не збираються (серед останніх “досягнень” – зараження банківських комп’ютерних мереж Лондона та Франкфурта у зв’язку з початком чемпіонату світу з футболу-2006 у Німеччині, масове зараження комп’ютерів у Китаї в 2007 році (через китайську версію Windows Vista).

Якщо раніше комп’ютерні віруси повністю відповідали своїй назві і могли потрапити до комп'ютера користувача разом з носієм (дискетою, компакт-диском і т.д), через комп’ютерну мережу або з повідомленням електронної пошти, то з розвитком електронних технологій віруси почали освоювати новий простір (мобільні телефони). До 2006 року під їх “зацікавленість” підпадали тільки потужні телефони – смартфони і комунікатори, але сьогодні від вірусів не застрахований будь-який мобільний телефон, обладнаний Bluetooth-модулем (bluetooth – технологія безпровідної передачі даних). Спочатку Bluetooth-протокол було задумано як безпечний вид зв’язку (шифрування, аутентифікація, контроль якості обслуговування та інші типи захисту). Але було допущено деякі недоробки та залишено “дірки”, що і дало поштовх для розвитку телефонних “розваг” – bluejacking та bluehacking.

Bluejacking – жартування над власниками мобільних телефонів, що підтримують технологію Bluetooth, шляхом передачі повідомлень з “нівідкіль”.

Bluehacking – метод зламування або викрадення інформації через протокол Bluetooth.

Зломник можете дзвонити з чужого мобільного телефона, передавати будь-які повідомлення у будь-яку точку світу, вкрасти всю інформацію з мобільного телефона, зняти гроші з рахунка, переслати віруси для телефона.

Існує декілька видів атак зломників через Bluetooth:

– BlueBug – дозволяє отримати доступ до виконання AT-команд (команди, які починаються з символів AT, що дозволяють керувати мобільним телефоном). За допомогою певних команд можна отримати повний доступ до телефонної книги, повідомлень та інше;
– BlueSmack – атака довгим пакетом перевірки з’єднання, за рахунок чого телефон може “зависнути” або самовільно перезавантажитись.
– BlueSnarf – використовується сервіс OPP (OB-EX Push Profile), що використовується для спрощення передачі файлів. Для доступу до сервіса не потрібна аутентифікація, і це надає можливість передачі команд копіювання інформації з телефона.

Якщо користувач хоче уникнути вищезгаданих проблем, то потрібно вмикати захист (якщо він є) Bluetooth та користуватись антивірусними програмами для мобільних телефонів.