АНАЛІЗ НЕБЕЗПЕКИ АПАРАТНИХ ЗАКЛАДНИХ ПРИСТРОЇВ

Гриньов Р.С.
Науковий керівник – к.т.н., доцент Сєвєрінов О.В
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, каф. Безпеки інформаційних технологій,
тел:+38 (057) 702-14-25)
e-mail: rost_grin@rambler.ru

Attacks on organizations using hardware embedded devices are a serious threat. Especially in Ukraine, where such things are still not widespread and are not perceived as a serious danger.

В даний час питання безпеки в сучасних операційних системах, захисту персональних комп’ютерів та корпоративних мереж від шкідливого програмного забезпечення та проникнень не втрачає своєї актуальності. Проведений аналіз показав, що тенденція глобального розповсюдження вірусів прихованих в неліцензійному програмному забезпеченні та масового зараження притаманна територіям з високим рівнем “піратства”. Ці атаки спрямовані на звичайних користувачів і зловмисник не має намірів отримати доступ до інформації якоїсь конкретної людини.

Існують методи, що дозволяють приховувати віруси в усіх типах виконуваних файлів, у текстових файлах та файлах формату PDF. Вірусні атаки спрямовані проти конкретних людей, компаній, регіонів, країн та об’єктів інфраструктури заздалегіть сплановані, чітко продумані та мають більш складний характер. Спочатку зловмисники збирають дані. Потім їх можуть використати, наприклад, для проведення поштової спам-розсилки. Електронний лист оформлюється спеціальним чином, наприклад, лист від департаменту безпеки з прикріпленим файлом, в якому зазначені зміни політики безпеки. За допомогою макровірусу, що міститься у прикріпленому файлі зловмисник може отримати доступ до конфіденційної інформації компанії, встановити додаткові шкідливі програми з метою контролю інформаційних потоків організації або вивести з ладу обладнання, що спричинить значні збитки. Однак подібні атаки можна легко виявити через те, що вони мають масовий характер. Крім того, уважні працівники, звернувшись в департамент безпеки, дізнаються, що оновлення політики безпеки не було. Це дозволить швидко локалізувати розповсюдження вірусу, виправити всі наслідки та провести інструктаж з персоналом, що підвищить рівень безпеки організації. Все це можливо, бо відомий час проникнення в систему, спосіб який використовувався і найголовніше, що відбувся факт проникнення.

Зловмисники можуть використовувати різноманітні методики соціальної інженерії. Шахраї можуть використовувати звичайні флеш

накопичувачі, CD диски з вірусним програмним забезпеченням. Часто використовуються запрограмовані мікроконтролери. Якщо замаскувати подібний пристрій під виглядом маніпулятора “миша”, клавіатури або флеш накопичувача, то існує імовірність, що ним скористається хтось із співробітників організації. Таким чином зловмисник зможе проникнути, навіть в ізольовану систему, що не має доступу до глобальної мережі. Захиститися від подібних атак можна за допомогою регулярних інструктажів. Варто розуміти, що велика кількість витоків інформації з організації може відбуватись через неправильну утилізацію обладнання або під час ремонту. Наприклад, коли до ремонту потрапив комп’ютер, на жорсткому диску якого є фінансова звітність або розробки нового проекту. Проте правильна утилізація і виключення схожих ситуацій не гарантує безпеку. В будь-якій організації може виникнути ситуація, коли виходить з ладу устаткування. Це може бути мережевий пристрій, клавіатура. Після ремонту або заміни звичайного маніпулятора “миша” ніхто не помітить в ній наявності зайвого мікроконтролера, що може виконувати шкідливі дії. Такі атаки досить специфічні і мало розповсюджені, проте є найнебезпечнішими. Послуги таких центів можуть дорого коштувати, а з точки зору звичайної людини маніпулятор “миша” або клавіатура не можуть становити небезпеки для персонального комп’ютера або організації.

Подібні апаратні закладки можуть бути досить різноманітними. Одні можуть мати бездротові інтерфейси, інші доступ до Інтернету, що дозволить зловмиснику під’єднуватися до них дистанційно. Більш прості варіанти запрограмовані на виконання певних дій. Такі пристрої можуть бути приховані в системному блоці комп’ютера, маршрутизаторі, периферійному та іншому обладнанні. Небезпека атак, що використовують подібні пристрої полягає у важкості виявлення факту проникнення.

Таким чином, для захисту організації від вірусів, витоку інформації та проникнень в систему недостатньо мати сертифіковану операційну систему, фаєрволи та антивіруси. Необхідно на регулярній основі проводити інструктажі з метою підвищення рівня обізнаності персоналу у методах захисту персональних та корпоративних даних та з метою формування базових знань принципів інформаційної безпеки. Працівники повинні знати як діяти під час інцидентів інформаційної безпеки, розуміти ступінь відповідальності та можливе покарання за порушення правил політики безпеки. Крім того, необхідно чітко контролювати доступ персоналу, а особливо сторонніх людей, до різних департаментів та устаткування.

Список джерел: 1. Гриньов Р.С. Шкідливий USB HID-емулятор // Радіоелектроніка та молодь у XXI столітті: між. форум. Харків, 2018. С. 120-121.