Аналіз ефективності протидії сучасних засобів захисту компаній HID-атакам

Ростислав Гриньов[1], Олександр Сєвєрінов[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: rost_grin@rambler.ru

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: oleksandr.sievierinov@nure.ua

Коротка анотація – Interesting vector of attacks is use USB HID emulators of the keyboard (and mice) in the case of standard USB flash cards. And if autorun.inf on a flash card we already have learnt to search and destroy somehow with HID emulators all is meanwhile bad.

Комп'ютерні віруси, вразливість, HID-атака, антивірус, операційна система, утиліта.

I. Вступ

Питання безпеки в сучасних операційних системах не втрачає актуальності. Існує безліч різних векторів атак. 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 [1].

II. Можливі сфери застосування шкідливих hid-пристроїв

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. Якщо замаскувати подібний пристрій під виглядом маніпулятора "миша", клавіатури або флеш накопичувача, то можливо, що ним скористається хтось із співробітників. Відомі випадки, коли такі пристрої надсилались поштою в якості сувенірів або просто "губилися" поблизу організацій, наприклад, на парковці. Зазвичай, досить високий відсоток користувачів, які не замислюються про справжнє призначення пристрою і покладаються в даному питанні виключно на його зовнішній вигляд [2]. І тому дуже часто вони з упевненістю підключать подібне обладнання до комп'ютера. При цьому, ні система, ні, наприклад, антивірус не помічають вторгнення, оскільки визначають його як звичайну клавіатуру.

У подібних ситуаціях 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.

HID, або Human Interface Device - тип комп'ютерного пристрою, який взаємодіє безпосередньо з людиною. Найбільш часто приймає від оператора вхідні дані і надає йому вихідні дані. Найпоширеніші типи HID-пристроїв - це клавіатура, маніпулятор "миша" і джойстик.

III. Засоби захисту сучасних компаній

Якщо розглянути комп'ютер користувача, то в якості суттєвих ознак, з точки зору забезпечення безпеки, необхідно враховувати: безпосередньо інформацію, що знаходиться в системі, антивірусне програмне забезпечення, брандмауер та засоби захисту операційної системи (захист компонентів ядра та системних файлів, розмежування доступу до файлів та ресурсів на підставі атрибутів, автентифікація та авторизація користувача). Однак ці засоби захисту не можуть виявити та протидіяти даній атаці. Якщо розглядати структуру організації, то до її суттєвих ознак можна віднести всі ознаки інформаційної моделі комп'ютера користувача а також: IDS, IPS, DMZ, сервер автентифікації та авторизації, пісочниці, honeypot, технологію розподілення та ізоляції мереж та інформаційних потоків на підставі типів та особливостей інформації, що циркулює. З точки зору засобів захисту та комп'ютерної системи HID-пристрої є повністю довіреними і в основному розглядаються як простий інтерфейс між користувачем і машиною, тому системи захисту організації не зможуть виявити таку атаку. Тому, коли до комп'ютера підключається нова клавіатура і маніпулятор "миша", система не запитує дозволу на їх установку, і драйвери найчастіше встановлюються автоматично. Така безмежна довіра може поставити під удар безпеку всієї системи.

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 [3]. Оскільки в Україні мала кількість сертифікованих

сервісних центрів, то в найближчі декілька років ця проблема може стати досить поширеною. Послуги таких центрів можуть дорого коштувати, а з точки зору звичайної людини маніпулятор “миша” або клавіатура не можуть становити небезпеки для персонального комп’ютера або організації. Крім того, звичайний майстер, якого викликали виправити несправності, може встановити схожий пристрій.

IV. Типи та особливості шкідливих hid-пристроїв

Подібні апаратні закладки можуть бути досить різноманітними. Одні можуть мати бездротові інтерфейси, інші доступ через Інтернет, що дозволить зловмиснику під’єднуватися до них дистанційно [4]. 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. Подібні пристрої можуть використовуватися зловмисниками для здійснення багатьох атак, бо можуть залишатися непоміченими роками.

За основу подібного шкідливого USB-пристрою ми візьмемо Arduino Leonardo Micro (рис. 1), так як дана плата має підтримку USB, достатню кількість пам’яті, невеликі габарити та низку вартість [5]. Прошивка може бути написана в середовищі розробки Arduino Development Environment. Саме з її допомогою можна редагувати і записувати програму в мікроконтролер. Розробка коду здійснюється за допомогою С-подібного синтаксису.

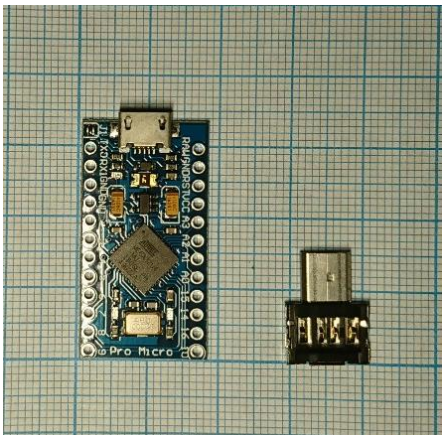

Рисунок 1 – мікроконтролер Arduino Leonardo Micro

Шкідливі пристрої подібного типу можуть виконувати різноманітні операції: від простого збору інформації про систему, викрадення паролів до повного контролю всієї системи і процесів з подальшим поширенням і зараженням нових пристроїв.

V. Захист від hid-атак

Існує кілька варіантів захисту від подібних атак:

1. Заборонити встановлення знімних пристроїв - це можна зробити за допомогою групової політики безпеки як для локальної машини, так і для робочих станцій в домені. Однак, при цьому буде не доступний Plug'n'Play.

2. Використовувати "білий список" - список довірених пристроїв. Слід врахувати, що пристрої ідентифікуються системою за рахунок ідентифікаторів Vendor ID і Product ID, які можуть бути запрограмовані зловмисником і повністю відповідати вже зареєстрованим в системі. Тому це не є абсолютним захистом.

3. Заборонити фізичний доступ до USB-портів. Проте таке рішення не є вдалим і може призвести до додаткових труднощів.

4. Використовувати для виявлення і блокування HID-емуляторів евристичні методи. Наприклад, ті, що грунтуються на аналізі зміни швидкості введення. Це найбільш раціональний і правильний підхід.

Висновки

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. Важливо пам'ятати, що навіть такий пристрій, як звичайний флеш накопичувач, може нести серйозну загрозу не тільки для персональних комп'ютерів, але і для більш складних обчислювальних систем.

Література

[1] The fighting HID emulator - URL: http://developers-club.com/posts/141838/.

[2] Evil USB the HID-emulator or it is simple Peensy- URL: http://developers-club.com/posts/141838/

[3] Гриньов Р.С. Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення / Р.С Гриньов, О.В. Севєрінов // Комп’ютерні та інформаційні системи і технології: між. науково-технічна конф. Харків, 2019. с. 75.

[4] Гриньов Р.С. Аналіз статистики та особливостей розповсюдження вірусів в Україні / Р.С Гриньов, О.В. Севєрінов // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління: між. конф. Харків, 2019. с. 100.

[5] Гриньов Р.С. Аналіз тенденцій вірусних загроз в Україні / Р.С Гриньов, О.В. Севєрінов // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління: між. конф. Харків, 2019. с. 120.