УДК 004.491.4 **DOI:10.30837/rt.2020.1.200.17**

Р.С. ГРИНЬОВ, О.В. СЄВЄРІНОВ, канд. техн. наук, А.В. ВЛАСОВ, канд. техн. наук.

МЕТОД ВИЯВЛЕННЯ ТА ПРОТИДІЇ ВІРУСАМ У ЗОБРАЖЕННЯХ ФОРМАТУ BMP

Вступ

З розвитком технологій нас оточує все більше технічних засобів, яким довіряється конфіденційна інформація. Створюються нові методики приховування і поширення комп'ютерних вірусів [1, 2]. Тому задача їх пошуку та протидії є актуальною не тільки для простих користувачів, а й для великих фірм та компанії. Для приховування комп'ютерних вірусів широко використовуються можливості стеганографії [3].

Саме тому, для забезпечення захисту даних користувачів було розроблено та досі створюються різні засоби захисту інформації. Наприклад, антивірусне програмне забезпечення, системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), брандмауери та фаєрволи [4]. Проте навіть цих засобів може бути недостатньо для того, щоб захистити дані.

Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP

Зловмисники додають до вірусів різні нові функції та розробляють нові методики приховування шкідливого коду, щоб подолати засоби захисту [5]. Зловмисники можуть впроваджувати вірусне програмне забезпечення в зображення для обходу антивірусних засобів, IDS/IPS і пісочниць. Перш ніж вірус буде запущений на комп'ютері співробітника, його проаналізує багато пристроїв (рис. 1).

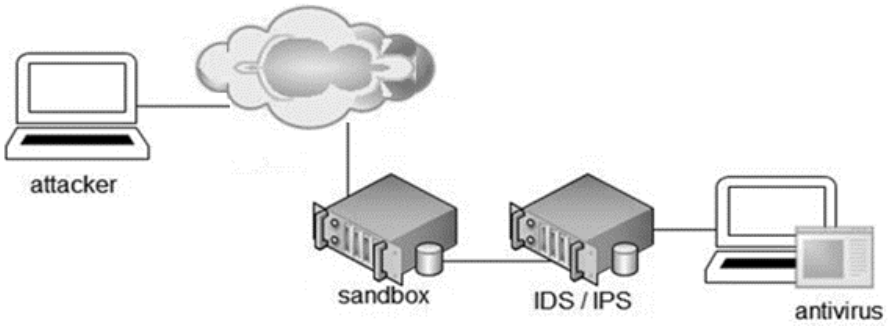

Рис. 1. Візуалізація шляху вірусу до цільового комп'ютера

Більшість методів аналізу файлів включають використання сигнатур вірусів і аналіз поведінки в пісочниці, а саме перевірку:

- поточного домену;
- запущених процесів;
- обсягу пам'яті;
- розміру диска;
- часу безвідмовної роботи.

Більшість пісочниць аналізуватимуть тільки виконувані файли, бібліотеки DLL, документи Word, аплети Java [6]. Більшість із засобів захисту просто не звертають уваги на зображення або інший безпечний тип файлу. Оскільки вважають, що немає причин витрачати процесорний цикл на аналіз зображення [7].

Так, наприклад, можна впровадити вірус у зображення формату BMP, таким чином, що користувач не помітить нічого підозрілого. Він не побачить ніяких дивних пікселів на зображенні. Справа в тому, що штучно зменшивши висоту зображення на декілька пікселів в заголовку можна приховати спотворені пікселі, але людина цього не помітить [8].

Ін'єкція можлива через те, що байти, які вказують на тип файлу, з яких і починається файл, BM в ASCII, в шістнадцятковому вигляді – 42 4D, при конвертації в інструкції асемблера не призводять до помилки виконання, а подальші 8 байт заголовка ніяк не впливають на інтерпретацію зображення [8]. Ці 8 байт можна заповнити будь-якими інструкціями асемблера, наприклад записати в них jmp-інструкцію, яка вкаже на вірус, що зберігається в зображенні. Щоб виконати код, що зберігається в зображенні, можна використати набір команд PowerShell.

Основна небезпека подібних зображень з вірусами полягає в тому, що для виявлення загрози необхідно використовувати нестандартні методи. Можна змінити налаштування засобів захисту, щоб вони перевіряли всі типи файлів, але це суттєво сповільнить або навіть повністю паралізує роботу всієї інформаційно-комунікаційної системи. Крім того, використання подібних інфікованих зображень може сильно ускладнити розбір інциденту інформаційної безпеки в організації. По-перше, системи безпеки можуть не відреагувати на вірус і виявити факт проникнення буде дуже складно. По-друге, якщо факт проникнення буде встановлений, буде майже неможливо з'ясувати як саме воно відбулося. Це обумовлено тим, що в першу чергу працівники відділу безпеки будуть з'ясовувати які виконувані файли, бібліотеки DLL, документи Microsoft Office, файли PDF потрапили в систему та використовувалися останнім часом. А через те, що не відома навіть приблизна дата проникнення, обсяг інформації, яку треба обробити значно зросте. В цьому випадку ніхто з працівників не буде досліджувати файли зображень.

Але аналіз показує, що віруси можуть заражати не тільки виконувані файли і динамічні бібліотеки, а й файли зображень, аудіо та відео.

Оскільки зображення неможна запустити як виконуваний файл, то і засоби захисту і технічні фахівці можуть легковажно ставитися до його вмісту та знехтувати цією загрозою. Однак такий файл може нести серйозну небезпеку. Необхідно уважно ставитися до налаштування систем запобігання вторгнень. І більш ретельно проводити розслідування інцидентів інформаційної безпеки.

Крім того, така вірусна атака може бути поєднана з HID-атаками, що робить її ще небезпечнішою [9]. Так, наприклад, зловмисник може запрограмувати мікроконтролер, щоб він при підключенні відкривав командний рядок, вводив та виконував команду PowerShell, що завантажить зображення та запустить вірус. Такий пристрій може бути замаскований під флеш-накопичувач, клавіатуру або інше периферійне обладнання [10].

HID-атаки

Використання HID-атак є рідкісним явищем для сучасного світу, хоча вони відомі досить давно. Шкідливі HID пристрої можуть бути різної форми та замасковані під різну апаратуру, проте всі вони виконують одні й ті ж завдання. Найчастіше вони виглядають, як звичайні флеш накопичувачі, проте насправді є HID пристроями і прикидаються в системі клавіатурою. Головна їх ідея полягає в тому, що клавіатура, як і решта HID пристроїв, є довіреними для системи та засобів захисту на відміну від виконуваних файлів, що перевіряються засобами захисту на наявність комп'ютерних вірусів. При підключенні подібного пристрою він починає виконувати запрограмовані дії. Наприклад, відкриває PowerShell та виконує команди, що завантажують зображення і виконують вірус, який знаходиться в ньому. З точки зору всіх систем захисту, це звичайний користувацький ввід команд через клавіатуру і він не є шкідливим, а пристрій – лише клавіатура. За допомогою шкідливих HID пристроїв зловмисник може скомпрометувати комп'ютерну систему без необхідності безпосередньо взаємодіяти з нею.

Методи виявлення вірусів у файлах зображень формату BMP

В першу чергу для протидії описаній в роботі атаці необхідно розроблювати нові засоби захисту та методи виявлення вірусів. А саме:

- необхідно, щоб антивірусні засоби захисту перевіряли файли зображень на наявність вірусів, в тому числі і за допомогою "масок";

- перевіряти файли зображень формату BMP на наявність будь-яких даних у зарезервованих полях заголовку відмінних від нулів. Якщо ці поля мають не нульові значення, це може означати, що у файл був впроваджений вірус;

- якщо поле “Size” в заголовку файлу не відповідає розміру файлу в байтах, це теж може свідчити про прихований шкідливий код;

- на основі кількості піксельних даних можна отримати інформацію про дійсний розмір зображення в пікселях, якщо він не відповідає ширині та висоті, які вказані в заголовку, це може свідчити про наявність вбудованого вірусу;

- також для виявлення шкідливого коду можна використовувати програми, що будуть визначати аномалії в зображенні. Так, при наявності великої кількості спотворених пікселів можна стверджувати про наявність в зображенні вірусу.

Суттєвим недоліком такого підходу є необхідність детального аналізу файлів та використання ресурсів обчислювальної системи. При великому навантаженні ІТС це може призвести до серйозних втрат працездатності та відмові в обслуговуванні. Крім того, для попередження подібних атак необхідно:

- чітко визначити перелік доступних інтернет-ресурсів для користувачів. Це унеможливить розміщення інфікованого зображення на web-ресурсах, до яких мають доступ зловмисники;

- фільтрувати та контролювати трафік організації. Якщо можливо, заборонити співробітникам завантажувати виконувані файли, скрипти, бібліотеки динамічних посилань (DLL). Крім того, завантажувати документи з невідомих джерел, що були створені в пакеті Microsoft Office та подібних, а також файли зображень формату BMP.

В ході дослідження було розроблено програму мовою Python, що перевіряє зарезервовані поля зображення BMP, поле SIZE, а також визначає справжню кількість пікселів та перевіряє зі значенням кількості пікселів по горизонталі та вертикалі, що зазначені в заголовку зображення.

При перевірці оригінального зображення не було виявлено жодних аномалій (рис. 2).

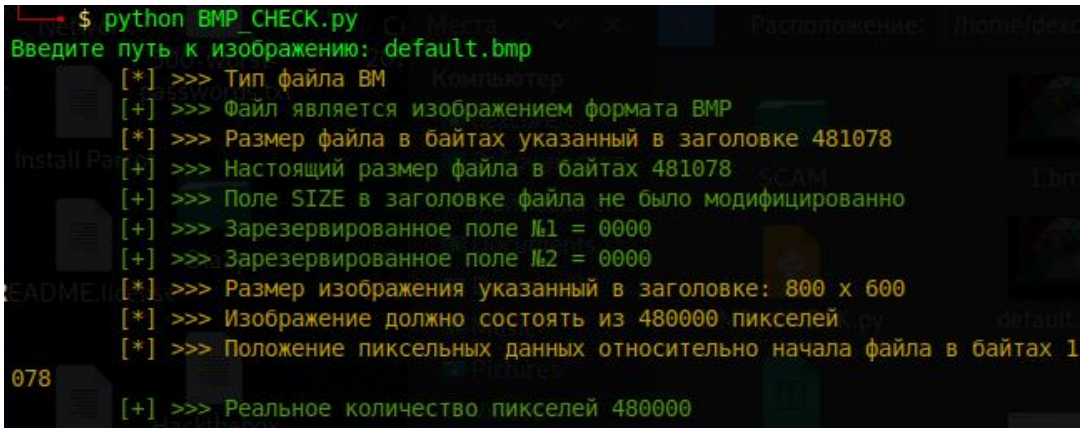

Рис. 2. Перевірка оригінального зображення

При перевірці інфікованого зображення були виявлені аномалії за ключовими ознаками (рис. 3).

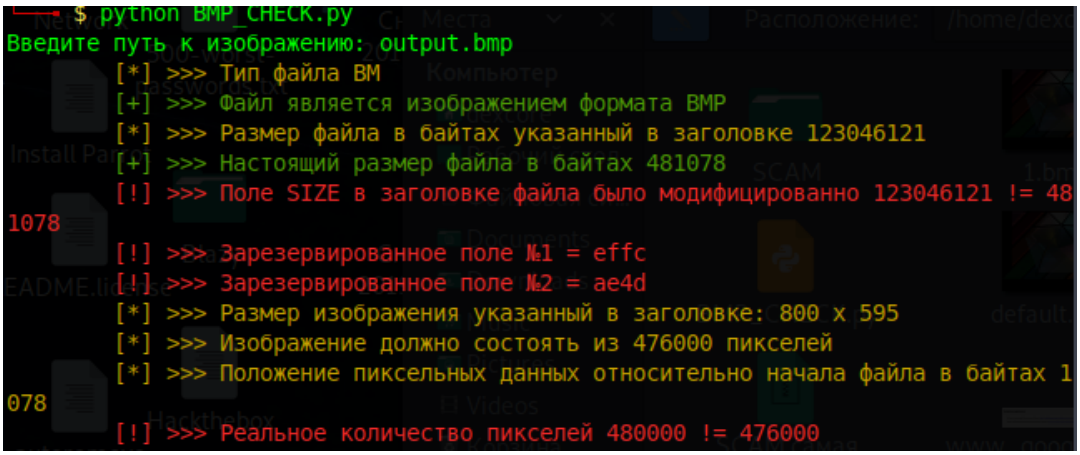

Рис. 3. Перевірка інфікованого зображення

Методи виявлення та протидії HID-атакам

Для виявлення та протидії HID-атакам необхідно:

- перевіряти придбане обладнання та обладнання після ремонту на наявність закладних пристроїв. Проводити періодичну перевірку існуючого обладнання;

- обмежити доступ до обладнання сторонніх осіб та працівників, які з ним не взаємодіють;

- необхідно, щоб при запуску PowerShell та CMD не тільки для адміністратора, але й будь-якого користувача було б необхідна обов'язкова автентифікація з використанням логіну та паролю;

- заборона на установку з'ємних пристроїв – реалізується за допомогою групової політики безпеки як для локальної машини та і для робочих станцій в домені. Однак при цьому не буде доступний "Plug'n'play";

- використання "білого списку" – списку довірених пристроїв. Однак слід враховувати, що пристрої ідентифікуються системою по зв'язці Vendor ID і Product ID, які можуть бути запрограмовані зловмисником і повністю відповідати вже зареєстрованим в системі. Таким чином, навіть блокування за "білим списком" не є абсолютним захистом;

- одним з найбільш ефективних засобів захисту від HID-атак є використання для виявлення та блокування евристичних методів аналізу, наприклад заснованих на аналізі зміни швидкості введення.

В ході дослідження була розроблена програма мовою Python, що виявляє та протидіє HID-атакам, аналізуючи швидкість введення тексту та її зміну. Якщо швидкість введення суттєво збільшилась і вона набагато вища за можливу людську, програма виявить атаку. Програма має чотири режими:

- коли атака буде виявлена, вона просто буде зареєстрована в журналі, без протидії;

- коли атака виявлена, кілька натискань клавіш будуть перервані (цього досить, щоб перервати будь-яку атаку, виглядає так, ніби нападник зробив помилку). Атака також буде зареєстрована в журналі;

- при виявленні атаки введення з клавіатури буде тимчасово відключено. Після того, як атака буде закінчена, введення з клавіатури знову буде дозволено. Атака також буде зареєстрована в журналі;

- при виявленні атаки блокує всі подальші натискання клавіш до тих пір, поки не буде введений правильний пароль. (Встановити пароль можна в файлі .conf). Атака також буде зареєстрована в журналі.

Програма не має графічного інтерфейсу. Після запуску програма функціонує як фоновий процес. Атака на комп'ютер під керуванням операційної системи Windows XP показана на

рис. 4. Варто зазначити, що до цієї атаки вразливі всі версії операційних системи сімейства Windows, Linux. MacOS також вразлива до цих атак.

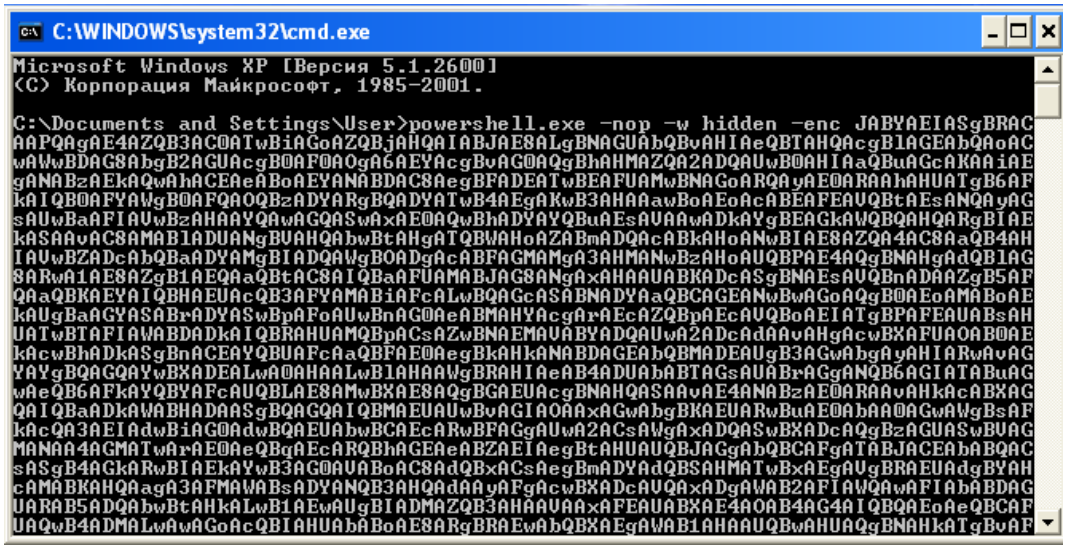

Рис. 4. Успішна атака на незахищену систему

Після запуску програми HID-атака була виявлена та знешкоджена (рис. 5).

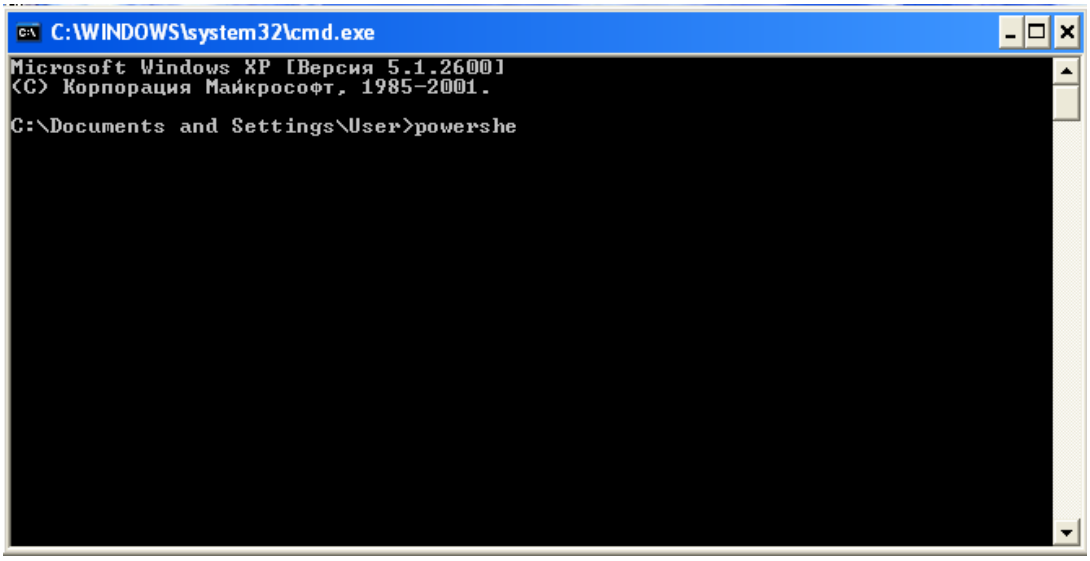

Рис. 5. Виявлена та знешкоджена атака за допомогою розробленої програми

Висновки

У ході досліджень розроблений та продемонстрований метод, що дозволяє виявити прихований вірус у зображеннях BMP. Створена програма для виявлення та протидії HID-атакам.

Проаналізувавши отримані результати, можна стверджувати, що даний метод виявлення прихованого вірусу дозволяє успішно виявити прихований шкідливий код у зображеннях формату BMP. Крім того, програма для захисту від HID-атак успішно виявила та знешкодила атаку.

За результатами випробувань можна стверджувати, що розроблені методи виявлення прихованого вірусного коду в зображенні формату BMP та протидії HID-атакам є більш ефективним для протидії цим атакам, ніж сучасні засоби захисту. Результати даної роботи мож-

на використовувати під час розробки засобів антивірусного захисту та комплексних засобів захисту ІТС та для їх модернізації з метою попередження подібних атак.

При цьому необхідно враховувати, що навіть звичайні файли з простою структурою без підтримки скриптів можуть становити серйозну загрозу. Тому необхідно розроблювати нові, більш ефективні засоби захисту.

Основна небезпека подібних зображень з вірусами полягає в тому, що для виявлення загрози необхідно використовувати нестандартні методи. Можна змінити налаштування засобів захисту, щоб вони перевіряли всі типи файлів, але це суттєво сповільнить або навіть повністю паралізує роботу всієї інформаційно-комунікаційної системи.

Список літератури:

1. Гриньов Р.С., Сєвєрінов О.В. Аналіз тенденцій вірусних загроз в Україні // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : міжнар. конф. Харків, 2019. 100 с.

2. Гриньов Р.С. Аналіз статистики та особливостей розповсюдження вірусів в Україні // Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : міжнар. конф. Харків, 2019.

3. Pare. Virus spread over networks: Modeling, analysis, and control : Ph.D. Electrical & Computer Eng / University of Illinois at Urbana-Champaign, 2018.

4. Jingwei LEI. Virus program detection method, terminal, and computer readable storage medium. United States, 2018. 19 c.

5. Wen-Kwang Tsao. Detecting malicious code in sections of computer files / Wen-Kwang Tsao, Pinghuan Wu, Zipan Bai. United States, 2018. 15 c.

6. Lubomir Sikora. Swarm Virus, Evolution, Behavior and Networking / Lubomir Sikora, Ivan Zelinka. Berlin, 2017.

7. Carey Parker. Computer Security. North Carolina USA, 2018.

8. Гриньов Р.С., Севєрінов О.В. Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення // Комп'ютерні та інформаційні системи і технології : міжнар. наук.-техн. конф. Харків, 2019. С. 75.

9. Гриньов Р.С., Сєвєрінов О.В. Шкідливий USB HID-емулятор // Радіоелектроніка та молодь у XXI столітті : міжнар. форум. Харків, 2018. С. 120-121.

10. Гриньов Р.С., Севєрінов О.В. Аналіз небезпеки апаратних закладних пристроїв // Радіоелектроніка та молодь у XXI столітті : міжнар. форум. Харків, 2019. С. 93-94.

11. Гриньов, Р. С., Сєвєрінов О. В. Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP // Радіотехніка. 2019. Вип. 198. С. 192-202.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 11.01.2020