УДК 004.056

ВПРОВАДЖЕННЯ КОДУ У ФОРМАТ PE-ФАЙЛУ

Рисований О.М., к.т.н., доц.
Національний технічний університет «Харківський політехнічний інститут»
Україна, Харків
rysov81524@gmail.com

Анотація. *В тезах розглянуто шляхи ін'єкції в PE-формат на прикладах DOS-заголовка, PE-заголовка та програмне втручання в кінець секції коду exe-файлу. Зроблено висновок про значення шляхів ін'єкції у PE-файл для ОС Windows 10/11 і їх роль у забезпеченні інформаційної безпеки.*
Ключові слова: *ін'єкція; PE-формат; DOS-заголовок; PE-заголовок*

Вступна частина. Актуальність теми впровадження в PE-заголовок (Portable Executable Header) обумовлена поруч факторів, пов'язаних з дослідженням, аналізом і безпекою програмного забезпечення. Завжди є інтерес використовувати службову частину файлу для своїх потреб – як правило для прикриття інформації.

На початку кожного exe-файлу знаходиться службова інформація, яка складається із заголовків. Розмір заголовків для архітектури мікропроцесора x64 дорівнює 1024 байт. Кожна секція має розмір не менше 512 байт і збільшується за мірою необхідності на це число.

Практична значимість впровадження в PE-заголовок для кібербезпеки передбачається наступним:

– впровадження коду або даних у PE-заголовок – це один із прийомів, які використовуються при аналізі шкідливого програмного забезпечення [1];

– знання цих методів необхідні для фахівців з реверс-інжинірингу, антивірусному аналізу та в судовій експертизі (форензиці) [2-3];

– дозволяє виявити спроби прихованого впровадження, поліморфізму або стеганографії у виконуваних файлах.

Крім того, упаковщики та захисники програм (наприклад, Themida, UPX, VMProtect) модифікують заголовки PE-файлів, додані метаданні або підписи.

Однак, в ОС Windows 10/11 ускладнюється контроль цілісності PE-файлів, що не дозволяє без змін використовувати відомі методи впровадження даних за допомогою PE-заголовка.

Метою роботи є аналіз PE-заголовка та пошук нових шляхів ін'єкції до нього для архітектури мікропроцесора x64 у середовищі програмування masm64.

Основна частина.

Впровадження коду в заголовок MS-DOS. Для впровадження коду в блок stub можна змінити стандартну заглушку " This program cannot be run in DOS mode" своїм текстовим повідомленням.

Алгоритм впровадження в заглушку (DOS Stub Message) з метою зміни системного повідомлення на інше повідомлення, може бути таким:

1. Відкрити файл на запис (GENERIC_READ або GENERIC_WRITE).
2. Створити відображення з правами PAGE_READWRITE.
3. Відобразити файл як FILE_MAP_WRITE.
4. Знайти адресу заглушки тексту (він іде в стандартний MS-stub після 0x4E).

5. Перезаписати його новим повідомленням.

Якщо заглушка короче, то необхідно додати команди NOP або нули.

Блок коду для виведення нового значення MS-stub на мові masm64 може бути таким:

```
invoke CreateFileA, addr filename, GENERIC_READ or GENERIC_WRITE, FILE_SHARE_READ, 0, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, 0
   mov  hFile, rax
invoke CreateFileMappingA, hFile, 0, PAGE_READWRITE, 0, 0, 0
   mov  hMapping, rax
invoke MapViewOfFile, hMapping, FILE_MAP_WRITE, 0, 0, 0
   mov  lpBase, rax
   mov rbx, lpBase
   lea r10, [rbx+4Eh] ; DOS stub для x64  - 0x4E
invoke lstrcpyA, r10, addr newmsg
invoke lstrcpynA, addr buf1, r10, 80
invoke MessageBoxA, 0, addr buf1, addr title1, MB_OK
invoke ExitProcess, 0
```

Після практичних прикладів зміни DOS-комірок з'ясовано, що вносити зміни в DOS-заголовок і DOS stub можна. Тільки не можна змінювати 2 комірки: MZ-сигнатуру та комірку з адресою 3Ch, в якій зберігається адреса знаходження PE-сигнатури.

Впровадження коду в PE-заголовок. У Windows 10/11 є комплекс заходів для захисту PE-заголовка, коли заголовки PE-файлів у пам'яті виконуються лише під час читання. Записати та зберігати дані в PE-заголовок та розраховувати, що програма потім їх запустить у завантаженій пам'яті – не вийде. Писати в PE-заголовок без зміни контрольної суми можна, але запустити такий файл не вдається. Операційна система блокує запуск таких програм.

Захист PE-файлів досягається за рахунок комплексних заходів, таких як шифрування виконуваного коду для запобігання антивірусному скануванню та аналізу, а також використання контрольної суми для підтвердження цілісності та справжності файлу.

Видається можливим після ін'єкції в PE-формат перерахувати контрольну суму і змінити її значення на нове.

Найпростіший шлях застосування PE-заголовка без зміни та підрахунку контрольної суми – це використання службових значень як основних даних своєї програми, наприклад, як пароля. Крім того, можна вільно використовувати службові осередки (причому вони мають різний розмір) для виконання різних операцій.

Формат PE-файлу складається як із заголовків, так і секцій. Втручання в секції можна здійснювати як у ручному режимі (з використанням зовнішніх програм, наприклад CFF Explorer), так і програмно.

При програмному втручанні найпростіше використовувати «латки». При цьому для запису даних в кінець секції даних іншого exe-файлу буде використано 2 файли:

– Patch.exe, який відкриває файл Target.exe та пише два числа в кінець файлу (наприклад, за межами останньої секції).

– Target.exe, який при запуску відкриває сам себе та зчитує ці числа з кінця.

У цьому випадку заголовок файлу не зіпсований і Windows запускатиме exe-файл на виконання.

Послідовність дій має бути такою:

1. Компілюється файл Target.asm у файл target.exe.

2. Компілюється файл Patch.asm у файл patch.exe.

3. Запуск файлу patch.exe. При цьому дані допишуться до кінця файлу.

4. Запускається файл target.exe та виводиться вікно повідомлення про результати виконання.

Програма Target.asm визначає кінець свого файлу та читає з нього дані.

Запис даних у кінець секції коду чужого exe-файлу та його читання є одним із найлегших завдань [1]. Записати в чужий exe-файл асемблерні інструкції не можна через не відповідність форматів. Писати можна лише коди чисел та інструкцій [2-3].

Висновки. У тезах показані прийоми впровадження в DOS-заголовок. Зроблено висновок, що вносити зміни в DOS-заголовок і DOS stub можна. Тільки не можна змінювати 2 комірки: MZ-сигнатуру та комірку з адресою 3Ch, в якій зберігається адреса знаходження PE-сигнатури.

При дослідженні PE-заголовка зроблено висновок, що писати в PE-заголовок без зміни контрольної суми можна, але запустити такий файл не вдасться. Операційна система блокує запуск таких програм. Для цього необхідно змінювати контрольну суму файлу.

Показано шлях програмного впровадження в кінці секції даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Рисований, О.М. (2025). *Реверсне програмування. Використання коду. Середовище програмування masm64: навчальний посібник для студентів спеціальностей 123 "Комп'ютерна інженерія", 125 "Кібербезпека".* Харків: «Слово». https://repository.kpi.kharkov.ua/handle/KhPI-Press/70274

[2] Рисований, О.М. (2024). *Методичні вказівки щодо виконання практичних та лабораторних робіт з курсу «Реверсне програмування. Антиналагоджувальні прийоми захисту від реверсу. Середовище програмування masm64: для студентів спеціальності 123 - «Комп'ютерна інженерія» всіх форм навчання.* Харків: НТУ «ХПІ». https://repository.kpi.kharkov.ua/handle/KhPI-Press/75508

[3] Рисований, О.М. (2024). *Реверсне програмування. Захист коду. Середовище програмування masm64: навчально-методичний посібник для студентів спеціальності 123 "Комп'ютерна інженерія" всіх форм навчання*. Харків: НТУ «ХПІ». https://repository.kpi.kharkov.ua/handle/KhPI-Press/79627

Rysovanyi O.M.

EMBEDDING CODE INTO PE-FILE FORMAT

Abstract. *The abstracts consider injection paths into the PE format using the examples of a DOS header, a PE header, and programmatic intervention into the end of an exe file code section.*

A conclusion is drawn about the significance of injection paths into the RE file for Windows 10/11 and their role in ensuring information security.

Keywords: *injection; PE format; DOS header; PE header.*