УДК 004.056.5
Зосенко К. В.[1], Зайко Т. А.[2]
[1]студ. гр. КНТ-127 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

ІНСТРУМЕНТИ ЗЛОМУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У процесі свого розвитку програмне забезпечення стало виходити за рамки технічних пристроїв і стало проникати в різні сфери людської діяльності. Програмне забезпечення управляє каналами постачання, надає доступ до глобальної інформації, дозволяє управляти заводами і фабриками і використовується для взаємодії з замовниками. Будь-яка помилка в такому програмному забезпеченні може призвести до тяжких наслідків. І саме такими помилками ПЗ користуються сучасні злочинці.

Злом програмного забезпечення був зведений в ранг мистецтва, це дійсно непросте завдання. Спочатку потрібно зрозуміти, яке завдання вирішує фрагмент коду. Часто це можна зробити тільки за результатами роботи. Іноді програмний код можна розділити на кілька фрагментів і вивчити їх окремо. Іноді призначення програмного коду визначається за допомогою некорректних вхідних даних. Цей код можна дизасемблювати і декомпілювати. Іноді з його допомогою код можна аналізувати або вивчити проект програми і архітектурні проблеми. Існує кілька типів програм, активно застосовуються для злому захисту програми.

Відладчики і дизасемблери традиційно використовуються в парі,

оскільки дизассемблер видає лише «чистий код», хоча сучасні дизасемблери здатні також розпізнавати виклики стандартних функцій, виділяти локальні змінні в процедурах і надавати інші подібні послуги. Користуючись дизассемблером, можна лише здогадуватися, які дані отримує та чи інша функція в якості параметрів і що вони означають. Щоб з'ясувати це, частіше за все потрібно вивчення якщо не всієї програми, то досить значної її частини.

Відладчики виконують інші функції: вони дозволяють аналізувати код в процесі його роботи, відстежувати і змінювати стан регістрів і стека, правити код на льоту - в загальному, спостерігати за діями програми і навіть активно в них втручатися.

Декомпілятори і вузькоспеціалізовані отладчики. З ростом потужності ПК широкого поширення набули компілятори, що створюють не "чистий" машинний код, а якийсь набір умовних інструкцій, який виконується за допомогою інтерпретатора.

Найчастіше буває потрібно дізнатися, які саме дії виконує програма, звідки вона читає і записує дані, які стандартні функції і з якими параметрами викликає. Отримати ці відомості допомагають утиліти моніторингу та API-шпигуни. Вони діляться на дві великі групи: відстежують сам факт виникнення будь-яких подій і дозволяють виявити один або кілька специфічних типів змін, що відбулися в системі за певний проміжок часу. Основна проблема при роботі з такими утилітами добре описується афоризмом: «Після - не означає внаслідок».

Існує також величезна кількість утиліт, які не вписуються в розглянуті вище категорії або потрапляють в кілька категорій відразу. Більш того, деякі утиліти, які можуть бути корисні для злому, створювалися для зовсім інших цілей. Як неможливо осягнути неосяжне, так і не можна описати всі програми, які застосовуються для злому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Росс Джей Андерсон Інженерія безопеки. Керівництво по створенню надійних розподілених систем / Ross J. Anderson, Cambridge, John Wiley & Sons, 2001. – 640 p.