АНТИВИРУСНЫЙ СКАНЕР ОБНАРУЖЕНИЯ ПРИЗНАКОВ В РЕ-СТРУКТУРЕ

Гавриленко С.Ю., Челак В.В.,
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Задача оперативного выявления вредоносного программного обеспечения, является актуальной, так как вирусы наносят убытки на десятки миллиардов долларов [1,2].

В докладе предложена модель антивирусного сканера, который проверяет программное обеспечение на наличие в нем ряда признаков вредоносного программного обеспечения.

Разработано приложение, которое позволило за счет анализа и реверс-инжиниринга выделить 20 различных признаков, извлекаемых из РЕ-структуры исполняемого файла, которые присущи данному семейству вирусов. Система принятия решений антивирусного сканера базируется на аппарате линейного программирования [3] с целевой функцией (1) и ограничениями (2),(3):

$$Z = x_1 + x_2 + \cdots + x_i + \cdots + x_n \to max, \quad (1)$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1i}x_i + \ldots + b_{1n}x_n \geq K_a, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2i}x_i + \ldots + b_{2n}x_n \geq K_a, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mi}x_i + \ldots + b_{mn}x_n \geq K_a, \end{cases} \quad (2)$$

$$\begin{cases} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1i}x_i + \ldots + b_{1n}x_n \leq K_b, \\ b_{21}x_1 + b_{22}x_2 + \ldots + b_{2i}x_i + \ldots + b_{2n}x_n \leq K_b, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mi}x_i + \ldots + b_{mn}x_n \leq K_b, \end{cases} \quad (3)$$

где K_a – левая граница значений на выборке, K_b – правая граница значений на выборке, x_i – переменная значимости i-го признака, b_{ij} – бинарные коэффициенты. Результатом использования симплекс-метода есть коэффициенты значимости признаков, полученные путем исследования образцов вредоносного программного обеспечения и используемые в системе принятия решения.

Литература:

1. Шелухин О.И. Обнаружение вторжений в компьютерные сети / Шелухин О.И., Сакалема Д.Ж, Филинова А.С.. – М.: Гарячая линия-Телеком, 2013. – 220 с.

2. Гошко С.В. Технологии борьбы с компьютерными вирусами / Гошко С.В.. – М.: Солон-Пресс, 2009. – 352 с.

3. Акулич И.Л. Математическое программирование в примерах и задачах / Акулич И.Л. – М.: Высшая школа, 1986. — 319 с.