

## СТАТИЧЕСКОЕ ДЕТЕКТИРОВАНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

**Д.Н. САЕНКО<sup>1</sup>, С.Ю. ГАВРИЛЕНКО<sup>2\*</sup>**

<sup>1</sup> магістрант кафедри ОТП, НТУ «ХПИ», Харків, УКРАЇНА

<sup>2</sup> професор кафедри ОТП, канд. техн. наук, НТУ «ХПИ», Харків, УКРАЇНА

\* email: 7573997@gmail.com

На протяжении последних десятилетий представление специалистов и пользователей о том, как должна выглядеть и работать «идеальная» антивирусная система, менялось. В общем и целом, процесс этого изменения можно представить, как отдельное развитие, конкуренцию и синтез двух концепций: статическое детектирование вирусов – по анализу файла в бинарном формате, динамическое детектирование вирусов – по их поведению в системе. В работе представлены результаты статического анализа 450 упакованных и не упакованных вирусов типа Worm, 3418 не упакованных вирусов типа Trojan, 3500 не упакованных вирусов типа Backdoor с целью выявления закономерностей, связанных с наличием определенных строк импорта и других строк в файле. Разработанное приложение позволило проанализировать импорт файла и PE- структуру файла. Полученные результаты позволили выделить наиболее часто используемые API-функции и строки, присущие данному типу вирусов, подсчитать их процентное соотношение. Было также проанализировано 690 безопасных приложений, выделены наиболее часто используемые API функции, подсчитано их процентное соотношение. Результаты анализа наиболее часто используемых API-функций приведены в табл.

Таблица 1 – Результаты анализа программного обеспечения

| Вредоносное программное обеспечение |              |                    |      |        | Безопасное ПО |          |
|-------------------------------------|--------------|--------------------|------|--------|---------------|----------|
| Тип вируса                          | Библиотека   | API функции        |      |        | Кол.          | %        |
|                                     |              | Функция            | Кол. | %      |               |          |
| Worm                                | kernel32.dll | GetModuleHandleA   | 247  | 85,17  | 306           | 43,83    |
| Worm                                | kernel32.dll | WriteFile          | 206  | 71,03  | 285           | 40,83    |
| Trojan                              | kernel32.dll | GetModuleHandleA   | 1270 | 67,589 | 306           | 43,83    |
| Worm                                | kernel32.dll | GetProcAddress     | 191  | 65,86  | 426           | 61,03    |
| Backdoor                            | kernel32.dll | GetModuleHandleA   | 736  | 65,83  | 306           | 43,84    |
| Trojan                              | kernel32.dll | GetModuleFileNameA | 1208 | 64,28  | 159           | 22,77937 |
| Worm                                | ADVAPI32.dll | RegCloseKey        | 178  | 61,37  | 318           | 45,55    |

Полученные результаты позволили выделить совокупность строк 78 и API-функции, присущих данному типу вирусов и сформировать его сигнатуру. Полученные данные могут быть использованы в дальнейшем для построения экспертной системы, позволяющей определить модификацию вредоносного обеспечения для рассмотренных классов вирусов.