ПОЛИМОРФНЫЕ ПРЕОБРАЗОВАНИЯ ВРЕДОНОСНОГО КОДА И ВОЗМОЖНЫЕ ПУТИ ИХ ОБНАРУЖЕНИЯ

Дроботун Е. Б.
Военная академия воздушно-космической обороны, г.Тверь

Дроботун Е.Б.
Военная академия воздушно-космической обороны

Термин «полиморфизм» (с греч. «многоформенность») применительно к компьютерным вирусам появился приблизительно в 1990 году. С того времени полиморфизм в вирусах прошел множество стадий своего развития: от простейшего побайтного шифрования до преобразований кода, использующих сложнейшие алгоритмы, в том числе криптографические.

Анализ работы большинства антивирусных программ показывает, что для гарантированного обнаружения компонентов вирусного или вредоносного кода используется сигнатурный поиск с жесткой привязкой к точке входа или физическому смещению в файле. Сигнатурой называется уникальная для каждого вируса последовательность байтов, однозначно его идентифицирующая. Сигнатура может быть сплошной (к примеру, DEh ADh FDh 3Eh F2h), либо разреженной (например, DEh … EDh … 3Ah C2h … EFh). Разреженная сигнатура иначе называется маской, поиск по разреженной сигнатуре – поиском по маске [1].

Для достижения приемлемой скорости сканирования антивирусные программы при сигнатурном поиске практически никогда не проверяют весь файл целиком, а ограничиваются лишь проверкой нескольких ключевых точек (например, в точке входа либо с привязкой сигнатуры к физическому смещению относительно начала файла).

Полиморфные вирусы – это достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, то есть, не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика (декриптора). К полиморфным вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи сигнатурного поиска или поиска по маске. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса.

Полиморфные вирусы активно развивались примерно до начала XXI века, однако затем произошел общий крен вирусописательства в сторону червей и троянов. Технология постоянной мутации кода для затруднения обнаружения антивирусными программами временно оказалась невостребованной.

Однако, начиная примерно с 2003 года, полиморфизм снова начинает привлекать внимание вирусного сообщества. Это было вызвано тем, что антивирусные программы все больше и больше совершенствовались, и уже стало нельзя использовать в качестве инструментов скрытия кода различные программы-упаковщики, которые были на тот момент излюбленным детищем вирусописателей.

В настоящее время практически все вирусы используют технику полиморфизма в том или ином виде для скрытия себя от антивирусных программ [2].

Для поиска и обнаружения вирусов, использующих ту или иные способы полиморфных преобразований, как правило, используется техника эмуляции процессора (называемая также технологией виртуальной машины). Антивирусная программа выполняет код в эмуляторе и после того как декриптор расшифрует основное тело вируса, далее применяет сигнатурный поиск. Это очень ресурсоемкая операция, и если применять ее для каждого исследуемого файла, процесс проверки будет занимать очень много времени.

Для сокращения времени проверки файлов, можно эмулировать выполнение исследуемых файлов, только для тех файлов, в которых предположительно обнаружены полиморфные преобразования. Для обнаружения полиморфных преобразований в файле можно проанализировать частоту появления отдельных байтов в файле, а также последовательности их появления и сравнив полученные при таком анализе значения со значениями частот появления отдельных байтов и следования их последовательностей в файлах, не подвергнутых полиморфным преобразованиям, сделать вывод о предположительном применении технологии

полиморфных преобразований. При этом, чем сильнее будут проявляться эти отличия тем с большей уверенностью можно говорить о применении полиморфных преобразований кода в исследуемом файле.

Литература

1. *Касперски К.* // Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 527 с.: ил.
2. *Касперски К.* // Записки исследователя компьютерных вирусов. – СПб.: Питер, 2005. – 316 с.: ил.