УДК 621.391.16

ОЦЕНКА ЭФФЕКТИВНОСТИ СИГНАТУРНЫХ МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

А. С. Вялых, С. А. Вялых

Воронежский государственный университет

Поступила в редакцию 21.04.2011 г.

Аннотация. В статье описывается новый подход к определению оценки эффективности сигнатурных методов обнаружения вредоносных программ.
Ключевые слова: вредоносная программа, информационная система, сигнатура, система массового обслуживания, сеть массового обслуживания.
Annotation. In article we consider the new approach to determination of a performance evaluation of signature methods of malware detection.
Keywords: malware, information system, signature, queuing system, network of mass service.

Для защиты современных информационных систем (ИС) от вредоносных программ (ВП) большинство пользователей используют антивирусы. Основным методом, с помощью которого антивирусы обнаруживают в ИС ВП, является метод сравнение с сигнатурами, хранящимися в базе соответствующего антивируса [1]. Как показывает статистика [2], за минуту в среднем появляется более 25 новых сигнатур ВП. Базы сигнатур ВП на серверах Лаборатории Касперского обновляются в среднем, каждый час [3], поэтому если в ИС базы сигнатур антивируса будут обновляться с такой же периодичностью, то до установки обновления ИС может быть поражена более чем 1500 новыми ВП. По умолчанию базы антивирусов в ИС обновляются раз в день, то есть до установки соответствующего обновления ИС может быть поражена более чем 36000 новыми ВП. Большинство ИС подключены к сети Интернет – основную среду распространения ВП, что серьезно увеличивает вероятность инфицирования. Кроме того, стоит отметить, что даже проникновение и активизация в ИС хотя бы одной ВП может привести к критическим ошибкам в работе ИС, ведущим к серьезным рискам. В связи этим актуальным является вопрос оценки эффективности сигнатурных методов обнаружения ВП.

ВП в ИС, защищаемой при помощи сигнатурных методов, может находиться в 4 состояниях:

1. ВП еще не создана.

2. ВП создана, но неизвестна для средств защиты, использующих сигнатурный метод.

3. ВП известна для средств защиты, использующих сигнатурный метод, но в базе сигнатур антивируса, установленного в ИС, отсутствует.

4. ВП, сигнатура которой есть в базе антивируса, установленного в ИС.

Процесс перехода ВП из одного состояния в другое можно представить в виде работы сети массового обслуживания (СеМО), состоящей из 2-х систем массового обслуживания (СМО), каждая из которых имеет бесконечное число каналов (рис. 1.).

В СеМО входит поток заявок (ВП) с интенсивностью λ. Данный поток с вероятностью 1 попадает в систему массового обслуживания (СМО) №1, которая имитирует процесс создания сигнатур. СМО №1 обслуживает каждую заявку (ВП) с интенсивностью μ_1, а n_1 – число заявок в этой СМО. Далее заявки с вероятностью 1 попадают в СМО №2, которая имитирует процесс добавления сигнатур в базу антивируса, установленного в ИС. СМО №2 обслуживает каждую заявку (ВП) с интенсивностью μ_2, а n_2 – число заявок в этой СМО. После обработки в данной СМО заявки выходят из СеМО. Под такими заявками подразумеваются ВП, сигнатуры которых есть в базе антивируса, установленного в ИС. Выбор в качестве входного потока пуассоновского потока вполне оправдан, так как фактически поток новых ВП представляет собой сумму потоков, порождаемых злоумышленниками, занимающимися созданием новых ВП. Их количество явно превышает 1000 [4], а в инженерной практике рекомендовано сумму

© Вялых А. С., Вялых С. А., 2011

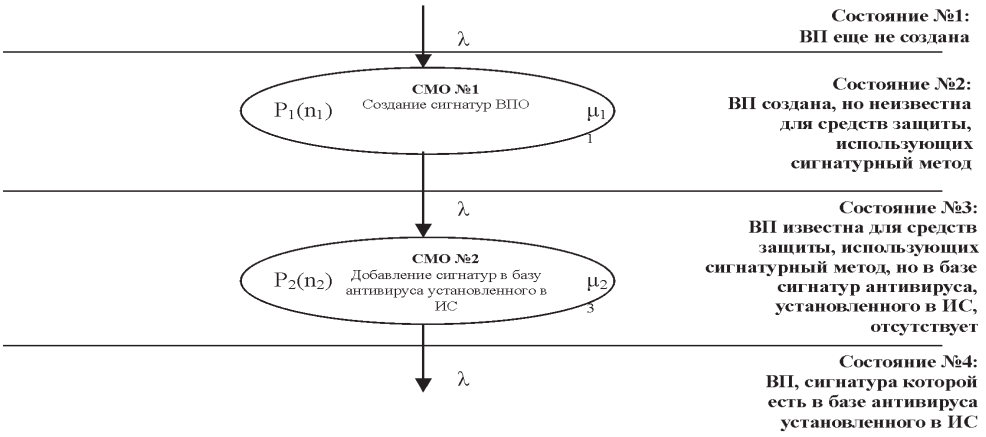

Рис. 1. Жизненный цикл вредоносной программы в информационной системе

уже из 5÷7 потоков считать пуассоновским потоком, если интенсивности этих потоков имеют одинаковый порядок и потоки независимы [5]. Предполагается, что в системе установился стационарный режим, и поток заявок, входящий в любую СМО, равен потоку заявок, выходящему из этой СМО. Вероятность отсутствия в ИС ВП, не детектируемых при помощи сигнатурных методов, будет равна вероятности отсутствия в СеМО заявок. Данная вероятность является грубой оценкой эффективности сигнатурных методов обнаружения ВП.

Вероятность того, что в СеМО, состоящей из M СМО, находится n заявок, можно рассчитать по формуле [6]:

$$P(n) = \prod_{i=1}^{M} P_i(n_i)\,,\ \sum_{i=1}^{M} n_i = n\,, \qquad (1)$$

где $P_i(n_i)$ – вероятность того, что в i-й СМО будет n_i заявок. В случае M=2, вероятность того, что в СеМО отсутствуют заявки, рассчитывается по формуле:

$$P(0) = P_1(0)P_2(0)\,, \qquad (2)$$

Вероятность того, что в i-й системе находится n_i заявок, равна [6]:

$$P_i(n_i) = P_i(0)\frac{\rho_i^{n_i}}{\beta_i(n_i)}\,,\ i = \overline{1,M}\,, \qquad (3)$$

где $P_i(0)$ – вероятность того, что в i-й системе отсутствуют заявки.

$$\rho_i = \frac{\lambda_i}{\mu_i},\ \lambda_i > 0,\ \mu_i > 0,\ i = \overline{1,M}, \qquad (4)$$

где λ_i – интенсивность потока заявок, входящего в i-ю СМО, а μ_i – интенсивность их обработки в этой СМО [6].

$$\beta_i(n_i) = \begin{cases} n_i\,!, n_i = \overline{0,c_i} \\ c_i\,!\,c_i^{n_i - c_i}, n_i \geq c_i \end{cases} \qquad (5)$$

где c_i – число каналов обработки в i-й СМО [6].

При использовании свойства $\sum_{n_i=0}^{\infty} P_i(n_i) = 1$, $n_i \geq 0$, $i = \overline{1,M}$ [4], получается:

$$P_i(0) = \frac{1}{\sum_{n_i=0}^{\infty}\frac{\rho_i^{n_i}}{\beta_i(n_i)}}\,,\ n_i \geq 0\,,\ i = \overline{1,M}\,. \qquad (6)$$

Так как число каналов обработки в каждой СМО бесконечно ($c_r = \infty$), то

$$\beta_i(n_i) = n_i\,!\ \lambda_i > 0,\ \mu_i > 0,\ i = \overline{1,M}, \qquad (7)$$

а вероятность отсутствия заявок в i-й СМО рассчитывается по формуле:

$$P_i(0) = \frac{1}{\sum_{n_i=0}^{\infty}\frac{1}{n_i\,!}\left(\frac{\lambda_i}{\mu_i}\right)^{n_i}}\ \lambda_i > 0,\ \mu_i > 0,\ i = \overline{1,M}\,. \qquad (8)$$

Можно показать, что с учетом формулы [7]:

$$e^x = 1 + \sum_{n=1}^{\infty}\frac{x^n}{n!}\,, \qquad (9)$$

выражение (8) принимает вид:

$$P_i(0) = e^{-\frac{\lambda_i}{\mu_i}}\ \lambda_i > 0,\ \mu_i > 0,\ i = \overline{1,M}\,. \qquad (10)$$

Интенсивность входящего в i-ю СМО потока равна [6]

$$\lambda_j = \lambda_0 a_j + \sum_{i=1}^{M}\lambda_i\Theta_{ij}\,,\ j = \overline{1,M}\,, \qquad (11)$$

где $\vec{\alpha}$, вектор, распределяющий вызовы поступивших заявок между M узлами сети, а Θ – квазистохастическая матрица, управляющая пере-

ходами между M узлами сети после завершения обслуживания заявки в очередном узле на ее маршруте.

Для СеМО, приведенной в этой статье (рис. 1), вектор $\vec{\alpha}$ равен

$$\vec{\alpha} = \begin{bmatrix} 1 & 0 \end{bmatrix}, \qquad (12)$$

а квазистохастическая матрица

$$\Theta = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \qquad (13)$$

Интенсивности входных потоков для 1 и 2 СМО будут равны соответственно

$$\lambda_1 = \lambda\,,\ \lambda_2 = \lambda\,, \qquad (14)$$

При подстановке (14) в (10), получаются формулы для вероятностей отсутствия заявок в 1 и 2 СМО соответственно:

$$P_1(0) = e^{-\frac{\lambda}{\mu_1}}\,,\ P_2(0) = e^{-\frac{\lambda}{\mu_2}}\,, \qquad (15)$$

При использовании (15), вероятность того, что в ИС отсутствуют не детектируемые сигнатурными методами ВП (то есть система защищена), получается равной

$$P(0) = e^{-\left(\frac{\lambda}{\mu_1}+\frac{\lambda}{\mu_2}\right)} \qquad (16)$$

Таким образом, получена формула, учитывающая возможные состояния ВП.

Интенсивность создания сигнатур и интенсивность их добавления в базу антивируса, установленного в ИС, не может быть больше, чем интенсивность создания новых ВП, так как не возможно создавать сигнатуры ВП быстрее, чем создаются эти ВП. Можно предположить, что интенсивность создания сигнатур и интенсивность их добавления в базу антивируса, установленного в ИС, равны интенсивности создания новых ВП, в этом случае

$$P(0) = e^{-2} = 0.135$$

Это максимальная вероятность того, что в ИС отсутствуют ВП, не детектируемые при помощи сигнатурных методов. Малое значение полученной вероятности показывает необходимость использования эвристических методов обнаружения ВП, таких, как эмуляция программного кода, виртуализация, hips-системы, поведенческий анализ, а также метод белого списка [5]. В [6] показано, что при помощи таких методов возможно определить до 68,5 % ВП, не детектируемых сигнатурными методами, то есть увеличить вероятность отсутствия недетектируемых ВП с 0,1 до 0,7. Стоит отметить, что только сигнатурные методы позволяют точно идентифицировать ВП и вылечить зараженную систему, поэтому рекомендуется обновлять базу сигнатур, используемую средствами защиты, не реже базы разработчика.

СПИСОК ЛИТЕРАТУРЫ

1. Обнаружение, основанное на сигнатурах // Википедия. – (http://ru.wikipedia.org/wiki/Обнаружение,_основанное_на_сигнатурах).

2. Облачные антивирусы – в теории и на практике. Часть 1. – (http://www.3dnews.ru/software/cloud-ativiruses-1/).

3. Лаборатория Касперского. – (http://www.kaspersky.ru/)

4. Leta о киберпреступности в России [Электронный ресурс] / «Лаборатория Касперского». – http://live.xakep.ru/blog/kaspersky_lab/592.html.

5. *Вентцель Е. С.* Теория случайных процессов и ее инженерные приложения. – Учеб. пособие для втузов. – 2-е изд. / Е. С. Вентцель, Л. А. Овчаров. – М.: Высш. шк., 2000. – 383 с.

6. *Башарин Г.П.* Лекции по математической теории телетрафика: учеб. пособие. – М.: Изд-во РУДН, 2004. 186 с.: ил. – (http://www.teorver.ru/newkatalog/1196719596.pdf)

7. Основы математического анализа : Учебник для физ. специальностей и специальности «Прикладная математика» ун-тов / В. А. Ильин, Э. Г. Позняк. — М. : Наука, 1980. – (Курс высшей математики и математической физики / под ред. А.Н. Тихонова [и др.] ; Вып. 2) .Ч. 2 .— 1980. — 447 с.

8. Антивирусная программам // Википедия. – (http://ru.wikipedia.org/wiki/Антивирусная_программа).

9. Результаты теста проактивной антивирусной защиты (июнь 2010) // Anti-Malware – (http://www.anti-malware.ru/proactive_test_2010).

Вялых Александр Сергеевич – аспирант кафедры информационных систем, Воронежский государственный университет. E-mail: alexandervyalih@gmail.com

Вялых Сергей Ариевич – кандидат технических наук, доцент кафедры информационных систем, Воронежский государственный университет. E-mail: vyalyh@govvrn.ru

Vyalih A.S. – post-graduate student, department of information systems, Voronezh State University. E-mail: alexandervyalih@gmail.com

Vyalih S.A. – Cand.Tech.Sci., senior lecturer, department of information systems, Voronezh State University. E-mail: vyalyh@govvrn.ru