ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
№ 1 ФИЗИКА 2004

УДК 004.056.57

Н.Г. БУЛАХОВ, Е.А. ПОДГОРНЫЙ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ИССЛЕДОВАНИИ ПРОЦЕССОВ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНОЙ СЕТИ КАК СЛОЖНОЙ СТРУКТУРЕ

Предлагается новый метод обнаружения вредоносного программного обеспечения саморазмножающегося в цифровых информационных сетях.

Сегодня вирусные атаки являются одной из первостепенных угроз информационной безопасности. Такие действия наносят финансовый ущерб, а также позволяют реализовать многие другие опасные угрозы. По сведениям аналитиков американской компании PC Tools Россия сейчас является лидером в распространении компьютерных вирусов, вредоносного и шпионского программного обеспечения [1]. Поэтому актуальная задача сегодня – исследование цифровых информационных сетей как сложных структур с целью разработки новых эффективных методов обнаружения компьютерных вирусов и червей.

Традиционно выделяется три основных класса методов обнаружения вредоносного программного обеспечения [2, 3]: сигнатурный, статистический и эвристический [4–6]. В отдельный класс следует выделить новый метод, основанный на анализе характеристик (а не содержимого) передаваемого по сети трафика, который практически одновременно предложен в работе [7] и авторами [8]. Сигнатурные, статистические и эвристические методы обладают существенными недостатками. Они требуют высоких затрат вычислительных мощностей аппаратного обеспечения, пропускают вирусы, не внесённые в сигнатурные базы антивирусного программного обеспечения, и существенно замедляют работу операционных систем. Это вызвано тем, что при использовании данных методов требуется анализировать исполняемый код непосредственно либо отслеживать поведение исследуемых программ в виртуальном окружении.

Для описания функционирования цифровых информационных сетей в период распространения компьютерных червей традиционно применяют эпидемиологические модели [9, 10]. Но они позволяют лишь наблюдать динамику роста числа заражённых узлов сети и не отображают важных сетевых параметров: способность сети передавать пользовательскую и служебную информацию и т.д.

Авторами разработана оригинальная модель функционирования цифровой информационной сети. Предложено рассматривать всю сеть как некое устройство, содержащее в себе коммутаторы, маршрутизаторы и оконечные станции. Тогда достаточно простой моделью, но которая учитывает особенности функционирования всей реальной сети (в том числе при пиковых нагрузках), способно служить сетевое устройство с обратной связью. Оно объединяет в себе функции маршрутизирующего оборудования и оконечных станций, являясь в этом смысле универсальным.

Указанное устройство имеет N входов и N выходов. Пара вход-выход образует подключение. Каждому подключению ставятся в соответствие два веса WO_i и WV_i, позволяющие дифференцировать загруженность выбранного канала, что отражает реальное разделение, например на магистральные и оконечные подключения сети. Внутри предлагаемого устройства каждому выходу соответствует очередь пакетов длиной M. Вес WO соответствует нагрузке канала за счёт обычных информационных пакетов, вес WV – за счёт саморазмножающихся пакетов, представляющих в данной модели компьютерных червей. Чтобы учесть динамику распространения саморазмножающихся пакетов, вводится обратная связь. Она осуществляется за счёт изменения веса WV при изменении числа саморазмножающихся пакетов на выходе устройства.

Найдены условия того, что в заданный такт времени на входе с номером n присутствует пакет, а если присутствует, то является либо саморазмножающимся, либо нет. В зависимости от весов WO_i и WV_i, соответствующих порту назначения с номером k, каждый пакет помещается в некоторую выходную очередь – согласно заданному критерию. Если же очередь переполнена, то пакет отбрасывается. Далее подсчитывается число пакетов каждого типа (NO_t и NV_t) на каждом выходе. Действие обратной связи (о которой говорилось выше) проявляется в коррекции весов WO_i и WV_i, согласно разработанному соотношению [11]. Очевидно, что предлагаемое устройство и его модель работают дискретно. Тогда логично использовать модель расширенного автомата, известную в теории автоматов.

Для проверки корректности предложенной модели выполнено компьютерное моделирование. Его результаты показывают, что модель отражает характер поведения разнородного трафика в проблемных сетях в согласии с экспериментальными данными [9], полученными в ходе анализа распространения реальных сетевых червей.

Модель [11] позволила оценить влияние распространения саморазмножающихся пакетов на количество и качество передачи информации по сети. Практически интересен тот существенный факт, что вторжение зловредного программного кода в цифровую информационную сеть изменяет ряд характеристик передаваемого по сети трафика, а по их численным значениям и типу динамики можно отследить потенциально опасную активность.

Характеристиками, пригодными для выявления такой активности являются: интенсивность пересылки отдельных пактов, интенсивность пересылки небольших очередей пакетов и интенсивность попыток установить соединение отдельными хостами, распределение IP- и MAC-адресов источника и назначения в передаваемых пакетах, размеры передаваемых пакетов, типы пакетов (принадлежность к определённым протоколам). Однако для достаточно надёжного детектирования вредоносной активности и сведения риска ложного срабатывания к минимуму в данном случае часто требуется некоторая «калибровка», составление сигнатур распространения известных червей. Это сужает область применения данных алгоритмов обнаружения сетевых атак и делает уязвимыми сети для новых (не внесённых в базу) червей. Авторы предлагают исключить параметры, варьирующиеся для конкретных реализаций червя, но добавить характеристики пересылки информационных пакетов внутри маршрутизаторов и коммутаторов: количество отбрасываемых пакетов в единицу времени, заполненность буферов пересылки, нагрузка оборудования.

Таким образом, можно увеличить количество параметров, идентифицирующих сетевую атаку и в случае обнаружения вредоносных пакетов, игнорировать такие пакеты, освобождая мощности оборудования для пересылки нормального трафика. После идентификации источника распространения зловредного трафика возможна его локализация и изоляция. Такого рода мониторинг потенциально опасной активности может производиться на небольшом количестве ключевых узлов сети без участия конечных пользователей. Это повышает надёжность системы обнаружения сетевых атак и предоставляет администратору возможность повысить управляемость сети.

СПИСОК ЛИТЕРАТУРЫ

1. Russia supersedes US & China as largest malware producer [Электронный ресурс]. – Режим доступа: http://www.pctools.com/news/view/id/197
2. Корт С.С. [Электронный ресурс]. – Режим дос-тупа: http://www.ssl.stu.neva.ru/sam/
3. Сердюк В. [Электронный ресурс]. – Режим досту-па: http://www.bytemag.ru/articles/detail.php?ID=9036
4. Матиас Р. [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/2006/10/3474604/
5. Chen W.H. Application of SVM and ANN for intrusion detection / W.H. Chen, Sh.H. Hsu, H.P. Shen [Электронный ресурс]. – Режим доступа: http://dx.doi.org/10.1016/j.cor.2004.03.019
6. Гудилин О.[Электронный ресурс]. – Режим доступа: http://www.viruslist.com/ru/analysis?pubid=189544544
7. Researchers invent system to control worms attacking computer networks [Электронный ресурс]. – Режим доступа: http://live.psu.edu/story/22189
8. Булахов Н.Г. Хасанов В.Я., Пойзнер Б.Н. // Проблемы инфор-мационной безопасности государства, общества и личности: Материалы 7-й Всероссийской научно-практической конференции (16–18 февраля 2005 г., г. Томск). – Томск: Изд-во ИОА СО РАН, 2005. – С 79–81.
9. Zou C.C., Gong W., Towsley D. [Электронный ресурс]. – Режим доступа: http://tennis.ecs.umass.edu/~czou/research/codered.pdf
10. Kim J., Radhakrishnan S., Dhall S.K. [Электронный ресурс] Режим доступа: http://ieeexplore.ieee.org/iel5/9617/30391/01401716.pdf
11. Булахов Н.Г., Пойзнер Б.Н., Турицин А.Л., Хасанов В.Я. // Материалы международной научной конференции "Статистические методы в естественных, гуманитарных и тех-нических науках" (апрель 2006 г., г. Таганрог). – Ч. 3. Таганрог: «Антон», ТРТУ, 2006. – С. 7–11.