УДК 621.394.6

ЗАЩИТА РАСПРЕДЕЛЁННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ ОТ САМОРАЗМНОЖАЮЩИХСЯ СЕТЕВЫХ ВИРУСОВ

Н.Г. Булахов

Предлагается принципиально новый метод обнаружения саморазмножающихся сетевых вирусов, основанный на анализе характеристик (а не содержимого) передаваемого по сети трафика.

В связи с бурным развитием и практически повсеместным использованием компьютерной техники в большинстве сфер человеческой деятельности информационная безопасность становится одним из наиболее востребованных направлений современных исследований. Постоянно совершенствуемые средства несанкционированного проникновения в компьютеры, порчи или массовой рассылки информации наносят серьёзный финансовый ущерб и заставляют тратить солидные деньги на разработку, приобретение и постоянное обновление защитного программного обеспечения. Поистине рассадником компьютерной «заразы» являются цифровые информационные сети. Именно их использование сделало перенос зловредного кода с одного компьютера на другой максимально быстрым, а участие человека при этом – необязательным. В руках злоумышленников появился мощный инструмент, позволяющий дистанционно организовывать отказы оборудования передачи данных или сетевых ресурсов, похищать конфиденциальную информацию, а также рассылать колоссальные объёмы рекламных писем, используя для всего этого тысячи компьютеров ничего не подозревающих пользователей. Поэтому актуальная задача сегодня – исследование цифровых информационных сетей как сложных структур с целью разработки новых эффективных методов обнаружения и нейтрализации вредоносного компьютерного программного обеспечения.

Традиционно выделяется три основных класса методов обнаружения вредоносного кода [1, 2]: сигнатурный, статистический и эвристический [3]. Они обладают рядом существенных недостатков, так как 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 этих методов требуется анализировать исполняемый код непосредственно, либо отслеживать поведение исследуемых программ в виртуальном окружении. Между тем, вирус, уже попавший на компьютер-жертву, может нейтрализовать работу антивируса до того, как он научится справляться с конкретно этой реализацией вредоносного программного обеспечения. К тому же некоторые вирусы «научились» скрывать своё присутствие в операционной системе, подменяя во время проверки файлы, содержащие вредоносный код, безобидными.

Автор предлагает принципиально иной метод обнаружения вредоносного программного обеспечения, основанный на анализе характеристик (а не содержимого) передаваемого по сети трафика. Этот метод пригоден для выявления различного рода сетевых червей, а также несанкционированных управляемых по сети программных закладок для массовой рассылки электронных писем или атак, направленных на отказ в обслуживании сетевого оборудования.

Автором была разработана модель функционирования цифровой информационной сети с учётом периодов пиковых нагрузок, вызванных распространением компьютерных червей и передачей паразитного трафика. Для проверки корректности предложенной модели выполнено компьютерное моделирование, результаты которого показывают, что модель отражает характер поведения разнородного трафика в проблемных сетях, согласуясь с экспериментальными данными [4], полученными в ходе анализа распространения реальных сетевых червей.

Модель [5] позволила оценить влияние распространения саморазмножающихся пакетов на количество и качество передачи информации по сети. Однако практический интерес представляет тот факт, что вторжение зловредного программного кода в цифровую информационную сеть изменяет ряд характеристик передаваемого по сети трафика, по которым можно отследить потенциально опасную активность.

Автором показано теоретически [5] и подтверждено экспериментально, что характеристиками передаваемого по сети трафика, пригодными для выявления потенциально опасной активности, являются: распределение IP- и MAC-адресов, TCP- и UDP-портов источника и назначения в передаваемых пакетах, размеры передаваемых пакетов и интенсивность пересылки широковещательного трафика. Эксперименты по распространению в локальной сети тестовых компьютерных червей показали, что в период активности вредоносного программного обеспечения в три раза и более увеличивается энтропия IP-адресов назначения, TCP- и UDP-портов источника в пакетах анализируемого трафика. В то же количество раз снижается энтропия IP-адресов источника, MAC-адресов, TCP- и UDP-портов назначения рассматриваемых пакетов. Другие известные методы обнаружения вредоносного программного обеспечения не позволяют выявить присутствие в сети компьютерных червей на столь ранних стадиях заражения. К подобным изменениям характеристик передаваемого по сети трафика приводит распространение заражённой машиной рекламных рассылок или осуществление атак, направленных на отказ в обслуживании сетевого оборудования.

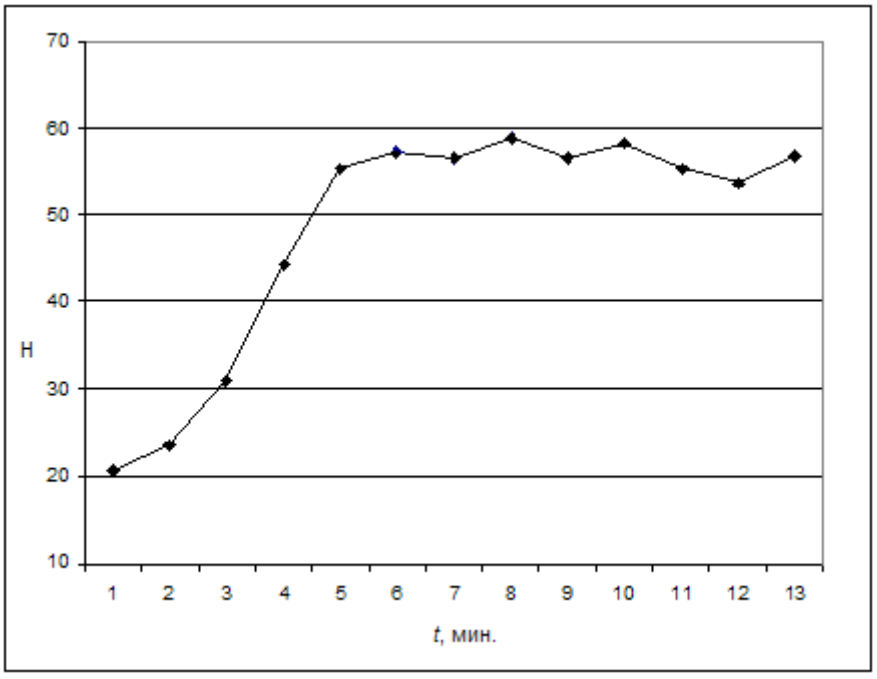

Рис. 1 – Изменение энтропии IP-адресов назначения в передаваемых по сети пакетах с течением времени при распространении сетевого вируса

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 большую гибкость, а также управляемость сети.

ЛИТЕРАТУРА

1. Корт С.С. Методы обнаружения нарушителя [Электронный ресурс]. – Режим доступа: http://www.ssl.stu.neva.ru/sam/
2. Сердюк В. Вы атакованы – защищайтесь! [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=9036
3. Матиас Р. Анализ поведения и эвристические методы выявления вирусов [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/2006/10/3474604/
4. Zou C.C Code Red Worm Propagation Modeling and Analysis / C.C. Zou, W. Gong, D. Towsley [Элек-тронный ресурс]. – Режим доступа: http://tennis.ecs.umass.edu/~czou/research/codered.pdf
5. Статистическая модель ЦИС, учитывающая возможность пиковых нагрузок / Н.Г. Булахов, Б.Н. Пойзнер, А.Л. Турицин, В.Я. Хасанов // Материалы международной научной конференции "Статистические методы в естественных, гуманитарных и тех-нических науках" (г. Таганрог, апрель 2006 г.). – Ч. 3. Таганрог: «Антон», ТРТУ, 2006. – С. 7–11.

Булахов Николай Георгиевич

Защита распределённых компьютерных систем от саморазмножающихся сетевых вирусов.

Предлагается принципиально новый метод обнаружения саморазмножающихся сетевых вирусов, основанный на анализе характеристик (а не содержимого) передаваемого по сети трафика.

Место работы: Томский государственный университет Радиофизический факультет кафедра Квантовой электроники и фотоники, аспирант

E-mail: nboolahov@yandex.ru

distributed computers protection from self-propagating network viruses

Nickolay Georgievich Bulakhov

Describe fundamentally new method of self-propagating network viruses detection. Method based on network traffic characteristic monitoring.