УДК 004.056.5
ББК 31

ПРОГРАММНЫЙ КОМПЛЕКС ОБНАРУЖЕНИЯ АТАК НА ОСНОВЕ АНАЛИЗА ДАННЫХ РЕЕСТРА

А.Е. Чурилина, А.В. Никишова

Разработан и описан программный комплекс обнаружения атак на основе анализа данных реестра. В качестве метода обнаружения атак предложены нейронные сети. Проведены экспериментальные исследования по обнаружению атак на информационную систему.

Ключевые слова: *программный комплекс обнаружения атак, системы обнаружения атак, нейронные сети, вирусные атаки, системный реестр.*

В настоящее время информационные технологии меняются настолько быстро, что статичные механизмы безопасности уже не обеспечивают полной защищенности системы. А потому систему защиты информации зачастую дополняют системами обнаружения атак. Система обнаружения атак (СОА) представляет собой программно-аппаратное обеспечение, контролирующее изменения, вносимые в какие-либо критичные данные информационной системы, и реагирующее при обнаружении признаков атаки [1]. Немаловажным для таких систем является свойство адаптивности, то есть возможности обнаруживать новые атаки и новые виды существующих атак.

Был проведен анализ существующих атак на информационную систему. Формы организации атак весьма разнообразны, но в целом все они принадлежат к одной из категорий: несанкционированный доступ к паролю, несанкционированное выполнение команд, нарушение прав доступа, атаки типа «отказ в обслуживании», «загрузка враждебного содержания».

Статистика показывает, что наиболее распространенными являются атаки, реализуемые с помощью загрузки враждебного содержания, например несанкционированных программ, таких как вредоносные программы («троянские кони»), вирусы, черви, макро-вирусы.

Операционные системы типа Microsoft Windows наиболее подвержены атакам типа «загрузка враждебного содержания». Многие несанкционированные программы (особенно «троянские кони») используют различные элементы системного реестра Windows для своего автоматического запуска в процессе загрузки операционной системы. Кроме этого большинство компьютерных вирусов, применяемых злоумышленниками для получения контроля над компьютером, используют реестр операционной системы Windows для перехвата некоторых системных функций или для автоматической загрузки тела вируса при загрузке компьютера. Кроме того, злоумышленник может удалить некоторые (или все) файлы реестра, что приведет к полной неработоспособности компьютера, или скопировать их к себе на компьютер, что даст ему возможность подобрать пароли к учетным записям пользователей.

Изменения, вносимые в реестр, могут привести к непоправимым последствиям для операционной системы или к получению злоумышленником административных прав. А потому необходимо анализировать данные реестра Windows для задачи обнаружения атак.

С целью выявления критичных для вопроса обнаружения атак областей реестра был проведен анализ его структуры и состава. Реестр Windows имеет иерархичную структуру и содержит 5 основных разделов: HKEY_CLASSES_ROOT, HKEY_CURRENT_USER,

HKEY_LOCAL_MA-CHINE, HKEY_USERS, HKEY_CURRENT_CONFIG [3].

Выяснено, что наиболее критичными разделами являются HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE.

По результатам анализа существующих атак и анализа системного реестра были выделены следующие критерии, по которым необходимо провести анализ существующих свободно распространяемых СОА (Snort, Bro, Prelude, OSSEC, STAT):

1. Уровень наблюдения за системой.

Различают системный и сетевой уровни. От уровня наблюдения за системой зависит скорость сбора информации, влияние системы на собираемую информацию, вероятность получения искаженной информации. Анализ атак показал, что целью большинства атак являются системные ресурсы, поэтому был выбран системный уровень.

2. Анализ реестра.

Из ряда источников данных на системном уровне по результатам предыдущего анализа был выбран реестр. Реестр является критически важным компонентом операционной системы, а значит анализ изменений, происходящих в нем, играет важную роль в процессе обнаружения атак.

3. Используемый метод обнаружения атак.

Современные вредоносные программы характеризуются постоянным возникновением новых типов и разновидностей старых типов этих программ. Поэтому разрабатываемая СОА должна использовать адаптивный метод обнаружения атак.

Анализ показал, что ни одна из существующих СОА не удовлетворяет критериям оценки. Необходимо создать СОА, удовлетворяющую всем приведенным выше критериям.

Для выбора метода обнаружения атак был проведен анализ следующих методов: анализ систем состояний, графы сценариев атак, нейронные сети, иммунные сети, экспертные системы, методы, основанные на спецификациях, сигнатурные методы, статистический анализ, кластерный анализ, поведенческая биометрия.

Для анализа использовались следующие критерии: адаптивность, вычислительная сложность, устойчивость, верифицируемость.

Критерии расположены в порядке убывания приоритета.

Анализ показал, что ни один из рассмотренных методов не удовлетворяет одновременно всем критериям анализа. Но в качестве метода, используемого в разработанном программном комплексе, выбраны нейронные сети. Обладая адаптивностью и будучи относительно устойчивыми, они имеют приемлемую для поставленной задачи обнаружения атак вычислительную сложность.

По результатам проведенного анализа был разработан программный комплекс обнаружения атак на основе анализа данных реестра. Его архитектура представлена на рисунке 1.

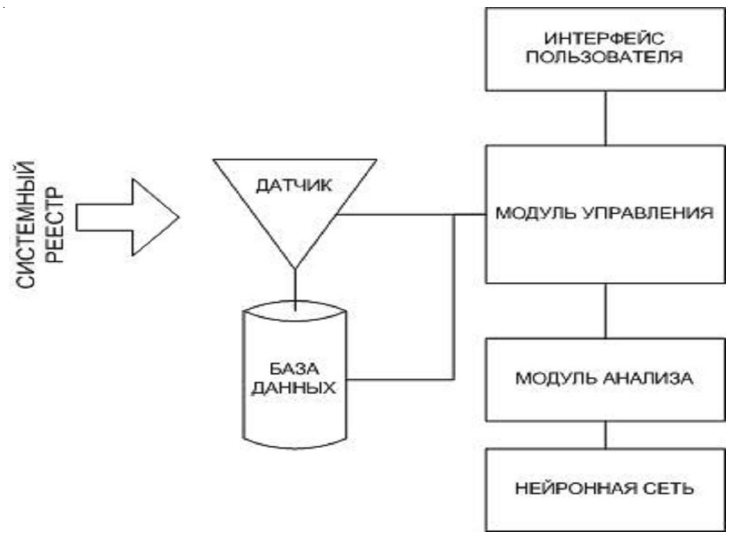

Рис. 1. Архитектура программного комплекса обнаружения атак

В состав программного комплекса обнаружения атак входит датчик, предназначенный для сбора информации из реестра, база данных, в которой хранится собранная датчиком информация, интерфейс пользователя, использующийся для взаимодействия специалиста по защите информации с элементами программного комплекса, нейронная сеть для распознавания атаки, модуль анализа и модуль управления, использующийся для координации работы отдельных элементов программного комплекса.

В качестве метода обнаружения атак нейронные сети обучаются на шаблонах нормального устоявшегося поведения. Был выбран тип нейронной сети многослойный персептрон с тремя входами и одним выходом. На первый вход подается информация о ветке реестра, на второй – время произошедшего события, на третий – путь к ключу. На выходе имеем вероятностную оценку возникновения атаки.

Специалист по защите информации может задать наиболее критичную ветку реестра, в которой будут отслеживаться изменения. Результаты выводятся в виде таблицы, где представлены:

- ветка реестра (название одного из корневых разделов реестра, в котором произошли изменения);
- время изменения (системное время события изменения ключа реестра);
- путь к ключу (путь к ключу, в котором произошли изменения).

Предусмотрена возможность построения диаграммы появления различных событий по времени.

Были проведены экспериментальные исследования. Предварительно в информационной системе с «устоявшимся» функционированием были собраны сведения о событиях, происходящих в реестре, для обучения нейронной сети. Была построена модель злоумышленника, которая атаковала информационную систему следующими «троянскими программами»: вирусная атака Trojan-Banker.Win32.Banker.cmb, вирусная атака Trojan.Win32.KillAV.br, вирусная атака Trojan.VBS.Seeker.g [2].

Результаты работы программного комплекса обнаружения атак приведены на рисунке 2.

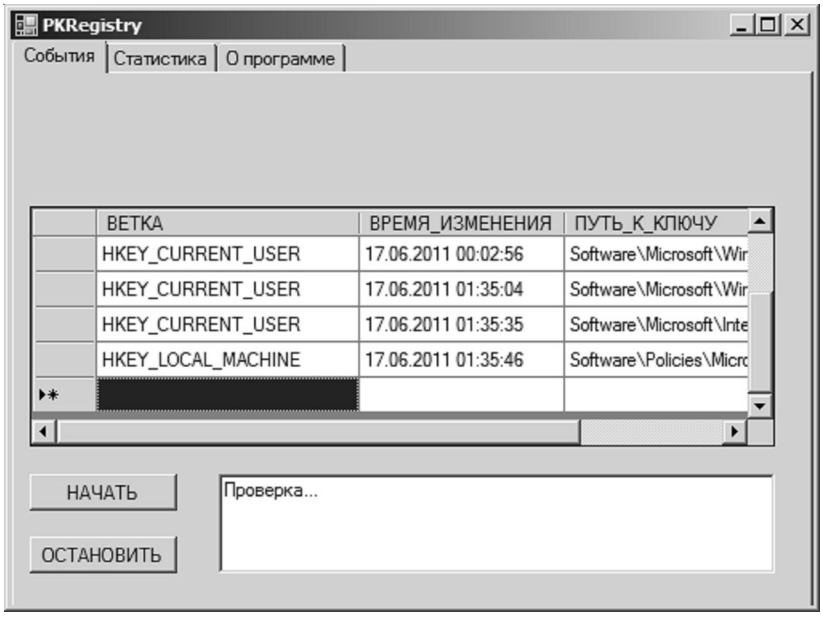

Рис. 2. Результаты работы программного комплекса обнаружения атак

Из рисунка 2 видно, что программный комплекс обнаружил изменения ключей в ветках реестра HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE, что не соответствует «нормальному» поведению информационной системы и свидетельствует об атаках Trojan-Banker.Win32.Banker.cmb, Trojan.Win32.KillAV.br и Trojan.VBS.Seeker.g.

СПИСОК ЛИТЕРАТУРЫ

1. Аргановский, А. В. Новый подход к защите информации – системы обнаружения компьютерных угроз. – Электрон. текстовые дан. – Режим доступа: http://www.jetinfo.ru/2007_detail. – Загл. с экрана.

2. Белоусов, С. А. Троянские кони. Принципы работы и методы защиты / С. А. Белоусов, А. К. Гуц, М. С. Планков. – Омск : Наследие : Диалог-Сибирь, 2003. – 33 с.

3. Колисниченко, Д. Секреты реестра Windows XP/Vista / Д. Колисниченко. – СПб. : БХВ-Петербург, 2008. – 17 с.

INTRUSION DETECTION PROGRAM COMPLEX BASED ON ANALYSIS OF REGISTRY DATA

A.Eu. Churilina, A.V. Nikishova

Developed and described intrusion detection program complex based on analysis of registry data. Neural networks were suggested as a method of intrusion detection. The experimental researches were held on the detection of attacks on information system.

Key words: *intrusion detection program complex, intrusion detection system, neural networks, virus attack, registry.*