$L_1(t)$ и $L_2(t)$ - потоки видеоданных соответственно от первой и второй видеокамеры системы видеоконтроля.

Полученное выражение позволяет определять уровень опасности ситуации на переезде для движения поездов, в зависимости от местоположения обнаруженного в зоне переезда постороннего объекта.

Вывод

В работе изложен подход к решению задачи определения уровня опасности ситуаций в опасной зоне железнодорожного переезда для движения поездов. В дальнейших исследованиях процесса видеоконтроля опасной зоны железнодорожных переездов предлагается рассмотреть:

• основные ситуации, возникающие в огражденной зоне переезда, для определения степени их опасности движению приближающихся поездов;

• особенности видеообнаружения посторонних объектов в зоне переезда с помощью детекторов активности в кадре изображения.

Литература

1. Обеспечение безопасности движения на переездах железных дорог мира. // Автоматика телемеханика и связь, 1997. – № 11– с.30-31.
2. Телевизионные системы контроля на Государственных железных дорогах ФРГ. // Железные дороги мир, 1985. – № 3 – с.28-36.
3. Грязин Г.Н. Системы прикладного телевидения: Учебное пособие для вузов. – СПб.: Политехника, 2000. – 277с.: ил.
4. Самсонкин В.Н., Друзь В.А. Метод статической закономерности в управлении безопасностью движения на железнодорожном транспорте. – Д.: ДонИЖТ, 2005. – 160с.
5. Инструкция по эксплуатации тормозов подвижного состава на железных дорогах Украины № ЦТ-ЦВ-ЦЛ 0015. Министерство транспорта Украины. – Киев: Транспорт Украины, 1997. – 133с.
6. Бойник А.Б. Теоретические основы эффективной эксплуатации систем управления ограждающими устройствами / Диссертация на соискание ученой степени доктора технических наук. – Харьков, 2003. – 336с.

УДК 681.3

НЕЙРОСЕТЕВЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО КОДА В ПРОГРАММНЫХ ОБЪЕКТАХ

А.С. Сапрыкин
Аспирант
Кафедра «Автоматизация проектирования вычислительной техники»
Харьковский национальный университет радиоэлектроники
пр.Ленина, 14, г.Харьков, Украина
Контактный тел.:8-068-603-00-81

В работе проанализированы современные проблемы антивирусных компаний и проблемы связанные с обнаружением модифицированного вредоносного кода. Разработан метод детектирования вредоносного кода с помощью эвристического анализатора на основе нейронной сети. Спроектирована модель системы принятия решений и проведены экспериментальные исследования по детектированию вредоносных объектов

1. Введение

За последние несколько лет количество вредоносных программ увеличилось в несколько десятков раз, при этом направленность деструктивного функционала приобрела криминальный характер. Число новых вирусов и троянских программ исчисляется сотнями ежедневно (рисунок 1) [1].

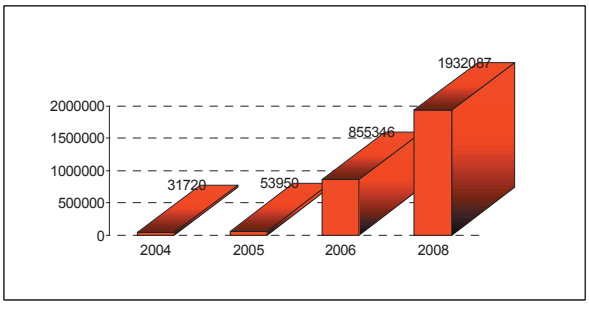

Рисунок 1. Ежегодный рост численности вредоносных программ

Все большее количество вредоносных программ создаются с одной целью – получение прибыли от различных незаконных видов деятельности, таких как похищение конфиденциальной информации, производственный шпионаж, создание и поддержка деятельности спам-бизнеса.

Вредоносные программы стали частью бизнеса, их создание и поддержка были поставлены на коммерческую основу, это в свою очередь положительно повлияло на качество применяемых в них технологий скрытия от обнаружения антивирусными программами.

2. Обзор литературы

Обзор литературы показал, что одна из наиболее эффективных и часто используемых технологий скрытия вредоносного кода – применение шифрования.

Новые модификации вредоносных программ появляются каждый день, при этом архитектура и функционал зачастую не претерпевают серьезных изменений. Различия между модификациями в большинстве случаев заключаются в использовании разных ключей и немного измененных алгоритмов шифрования [2].

Аналитикам антивирусных компаний приходится добавлять каждую новую модификацию в базы и выпускать их срочным обновлением, в то время как большое количество компьютеров уже оказывается зараженными.

Это происходит по причине недостаточной эффективности применяемых сегодня эвристических анализаторов - средств распознавания неизвестных модификаций.

Частично защитить от заражения новыми модификациями могут средства проактивной защиты антивирусных программ, однако и они имеют ограничения, так как настроены на распознавание некоторых общих типов вредоносного поведения. Основным способом выявления большинства компонентов таких вредоносных программ все еще является сигнатурная проверка.

Таким образом, появилась необходимость в разработке нового эвристического метода, который бы смог эффективно распознавать схожие модификации вредоносных программ.

Метод должен быть основан на анализе поведения и действовать в обход шифрования на более высоком уровне [3].

Данный метод позволит защитить компьютерные сети проактивно, без необходимости обновления антивирусного ПО, а также позволит уменьшить время реакции антивирусных компаний на появление новых вирусных эпидемий.

3. Цель и задачи исследования

Цель исследования – разработка эффективного метода детектирования модифицированного вредоносного кода.

Задача исследования – разработка модели эвристического анализатора на основе нейронной сети.

Объект исследования – вредоносный код в исполняемых PE EXE – файлах.

4. Система автоматического создания вирусов

Система, обнаруживая факт детектирования вируса антивирусными программами, автоматически генерирует модификацию вредоносной программы с измененным алгоритмом шифрования и автоматически запускает ее в Интернет для нового заражения пользователей [3].

Таким образом, вирусописатели, всегда оказываются впереди антивирусных компаний, примером такой программы является почтовый червь Email-Worm.Win32.Warezov или троянская программа, предназначенная для похищения конфиденциальных данных Trojan-PSW.Win32.LdPinch.

Система состоит из следующих модулей:

Модуль проверки детектирования.

Его функцией является определение факта детектирования конкретным антивирусом текущей модификации вируса.

Полиморфный мутатор.

При получении информации о том, что текущая модификация вредоноса уже добавлена в антивирусные базы, данный модуль производит мутацию вирусного кода: шифрует тело вредоносной программы новыми ключами шифрования и с применением новых алгоритмов.

Новые алгоритмы генерируются автоматически на основе правил перестановки и замены операций из некоторого ограниченного набора. Таким образом, сразу после выхода обновления со стороны антивирусной компании выходит и новая модификация со стороны вирусописателей.

Система доставки новых модификаций пользователям обычно является роботом для рассылки писем электронной почты содержащих во вложениях новосозданные модификации вредоносных программ [4].

Алгоритм работы данной системы приведен на рисунке 2.

По данным Лаборатории Касперского, количество выпускаемых в месяц модификаций червя Worm.Win32.Warezov составляет более сотни и примерно 3-4 модификаций в день [1].

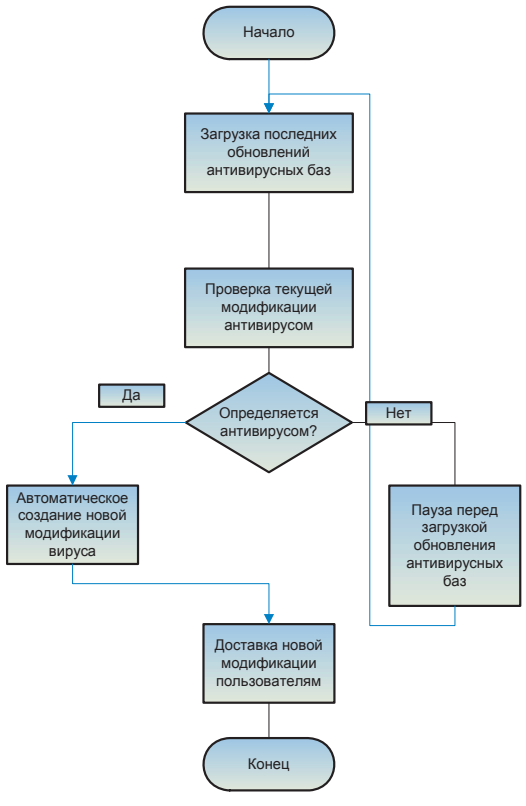

Рисунок 2. Алгоритм работы системы автоматического создания вирусов

5. Модель эвристического анализатора

Для организации метода детектирования нужно выполнить следующие действия:

1. Произвести запуска под API - монитором или Эмулятором вредоносный объект.

2. Получить Лог- файл, содержащий последовательность вызова функций и передаваемые аргументы.

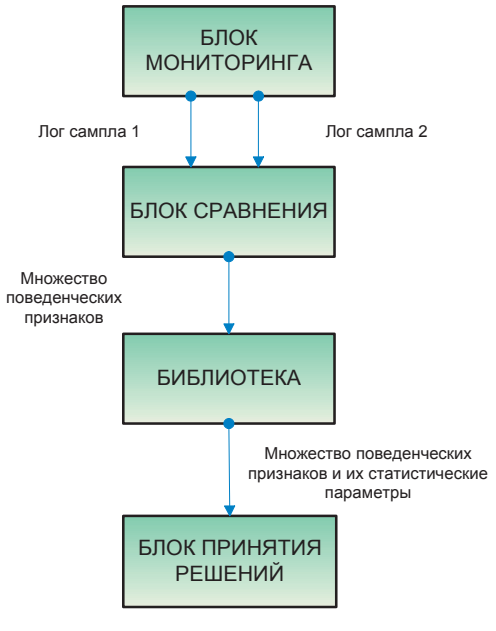

Рисунок 3. Схема системы принятия решений

3. Выполнить процедуру анализа на ”схожесть” функционального поведения программного объекта с данными известными о функциональном поведении других объектов хранимых в библиотеке.

4. Выделить поведенческие группы среди программных объектов, имеющих вредоносное схожее поведение и сделать вывод о принадлежности/непринадлежности рассматриваемого образца к некоторому семейству вредоносных программ.

Схема анализатора представлена на рисунке 3.

Блок мониторинга. Функцией данного блока является мониторинг поведения вредоносных и не вредоносных объектов с целью получения протокола их работы (последовательностей вызова API функций и переданных им аргументов).

Блок сравнения. Данный блок принимает протоколы работы нескольких образцов от блока мониторинга и сравнивает их. Результатом работы данного блока будет множество одинаковых фрагментов в протоколах разных образцов одного семейства (далее «признаков»).

Библиотека. Данный блок хранит в себе все признаки, выявленные блоком и ведет статистику их встречаемости. На основе данной статистики каждому признаку присваивается рейтинг, характеризующий встречаемость данного признака, т.е. фрагмент, который был найден в протоколах всех образцов будет иметь наибольший рейтинг, а фрагмент, который найден в наименьшем количестве образов – наименьший. Кроме того, так же ведется инкрементальный рейтинг новизны признаков, если новый фрагмент был найден – ему присваивается рейтинг N+1, где N – рейтинг найденного перед ним признака.

Блок принятия решений. Основной компонент системы, функция данного компонента – принятие решения о принадлежности/непринадлежности рассматриваемого образца к некоторому семейству вредоносных программ и ведение базы знаний.

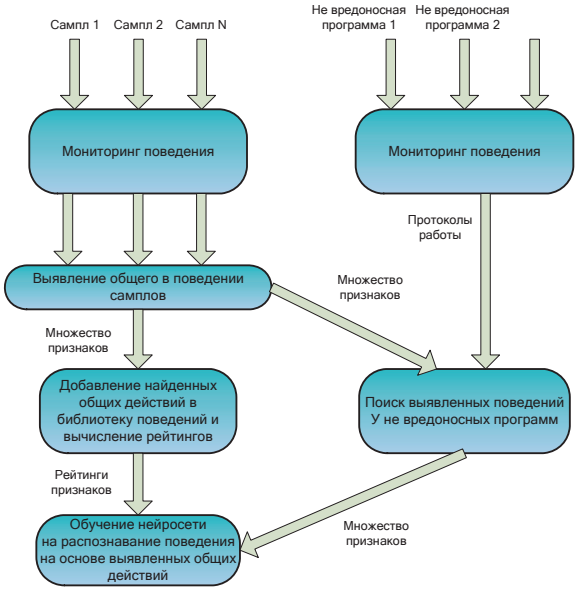

Рисунок 4. Движения данных

Блок состоит из нейронной сети, количество задействованных нейронов определяется количеством най-

денных признаков и должно изменяться динамически, в зависимости от того, каким количеством признаков будут обладать все образцы, на этот показатель будут влиять функциональные тенденции в новых модификациях [5].

Схема движения потоков данных представлена на рисунке 4.

Блок работает в двух режимах – обучение и детектирование. При обучении на вход блока поступают множества рейтингов встречаемости признаков. Данные берутся из вредоносных образцов и невредоносных программ, после чего разбиваются на группы по своей новизне. Для каждой группы составляется своя нейросеть, количество входов нейронов которой равно количеству признаков в группе, после чего нейросети предъявляются значения рейтингов встречаемости признаков, которые были найдены в образцах, на которых она обучается. Если рейтинг встречаемости всех элементов в группе признаков со временем становится слишком низким и показатель новизны группы слишком мал – группа удаляется, а признаки, имеющие наивысший рейтинг встречаемости в группе будут перенесены в новую группу.

Рисунок 5. Алгоритм добавления новых признаков в библиотеку

Таким образом, устаревшие данные или случайные неверные признаки со временем не будут браться в расчет для того, чтобы сделать более точным определение новых модификаций. В свою очередь, при определении новой модификации – протокол будет повторно рассмотрен более детально на предмет выявления новых возможных признаков. При выявлении новых признаков приоритет будет у функций, изменяющих состояние системы (таких как работа с реестром, файловой системой или сетью). Новые признаки будут добавлены в библиотеку, в случае, если они будут ошибочные, их рейтинг встречаемости будет понижаться, и, со временем, они будут ликвидированы, алгоритм работы показан на рисунке 5.

6. Экспериментальные исследования

Для решения задачи обнаружения вредоносного кода рассмотрим многослойный нелинейный персептрон с обратным распространением ошибок. Многослойный персептрон представляет собой нейронную сеть, состоящую из нескольких слоев. Их число, а также количество нейронов в каждом слое зависит от поставленной задачи. В нашем случае применяется три слоя:

1. Количество нейронов в первом входном слое равно количеству признаков.
2. Количество нейронов в последнем выходном слое равно одному.
3. Количество нейронов в среднем внутреннем слое выбирается как среднее арифметическое между количествами нейронов во входном и выходном слоях [6].

Выполняем обработку данных с помощью многослойной нейронной сети и делаем вывод о принадлежности/ непринадлежности данного образца к некоторому семейству вредоносных программ (рисунок 6).

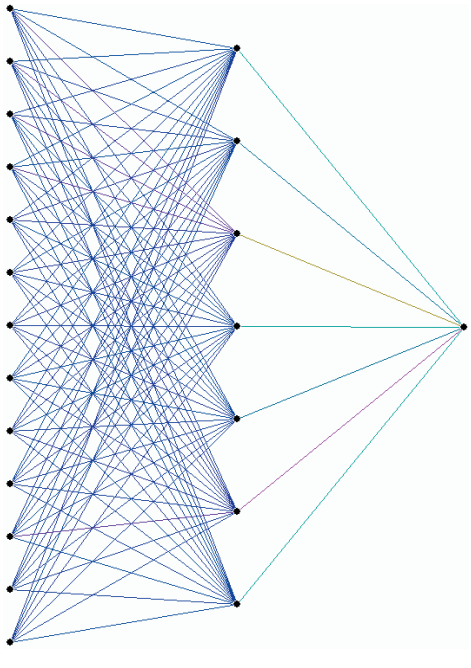

Рисунок 6. Нейронная сеть для детектирования семейства Trojan-PSW.Win32.LdPinch

Используя аналитическую платформу Deductor, проводим эксперимент, в котором, изменяя значения входных полей (рейтингов признаков) нейронной сети, наблюдаем за изменением значений на выходе (рисунок 7).

Поле	Значение
Входные	
9.0 признак1	0
9.0 признак2	1
9.0 признак3	1
9.0 признак4	0,83
9.0 признак5	0,66
9.0 признак6	0,5
9.0 признак7	1
9.0 признак8	0,83
9.0 признак9	0,83
9.0 признак10	0,83
9.0 признак11	0,83
9.0 признак12	0,83
9.0 признак13	0,5
Выходные	
Вердикт	True

Рисунок 7. Распознавание Trojan-PSW.Win32.LdPinch.aate

7. Выводы

Разработана система принятия решений на основе многослойного персептрона, позволяющая с высокой долей вероятности выполнять задачу обнаружения модифицированного вредоносного кода в программных объектах.

Система способна детектировать новые вредоносные программы без внесения дополнительных поведенческих признаков в обучающую выборку, тем самым защищать пользователей от современных вирусных атак.

Применение упаковки и шифрования не оказывает значительного влияния на качество распознавания.

Разработанный метод детектирования может найти промышленное применение в средствах антивирусной защиты, также метод позволит значительно увеличить скорость реагирования на возникающие эпидемии полиморфных вирусов.

7. Литература

[1] http://www.kaspersky.ru

[2] Касперски К. Записки исследователя компьютерных вирусов. – СПб.: Питер,2005.–316 с.

[3] Касперски К. Техника и философия хакерских атак – записки мыщ'а.–Салон – Пресс, 2004. – 272с.

[4] Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 527 с.

[5] Saprykin Aleksandr, Kiktenko Vitaly, Galagan Sergey, Kunitsky Artem. Diagnosis method of malicious code in executable files, Proceedings of the 5th East-West Design and Test Workshop, Yerevan, Armenia, 7-10 September 2007.

[6] Руденко О. Г., Бодянский Е. В. Искусственные нейронные сети: Учебное пособие. – Харьков, 2005. – 408 с.