Комбинирование методов Data Mining для статического детектирования Malware

Комашинский Д.В., Котенко И.В.
Лаборатория проблем компьютерной безопасности, СПИИРАН
{komashinskiy, ivkote}@comsec.spb.ru

Ввиду объективных причин проблема противостояния вредоносному программному обеспечению (далее – malware, от англ. “malicious software”) в условиях использования современных информационных технологий стоит достаточно остро. Существует большое количество методов его обнаружения, начиная с традиционного поиска сигнатур и заканчивая продвинутыми эвристическими подходами, позволяющими выявлять ранее неизвестные варианты вредоносного программного обеспечения за счет формирования обобщенных спецификаций признаков, характерных для тех или иных семейств вредоносных программ.

К сожалению, технологии, используемые при разработке вредоносного кода, тоже не стоят на месте и имеют даже опережающую по сравнению с традиционными областями разработки программного обеспечения тенденцию к применению новых инструментальных и алгоритмических средств. Это объясняет текущее состояние дел в данной области – несмотря на очевидные успехи исследовательского и инженерного сообществ на данной стезе, причин утверждать то, что в ближайшем времени следует ожидать появления какого бы то ни было радикального перелома в области противодействия malware, к сожалению нет. Данный факт стимулирует дальнейшее развитие подходов к выявлению malware и, в том числе, ставит пред исследователями задачу практического обоснования применимости в области разработки эвристических подходов детектирования так называемых методов интеллектуального анализа данных (далее Data Mining, DM).

Следует отметить, что подобная постановка вопроса не нова – первые публикации, посвященные данной тематике, появились более десяти лет назад. Регулярно исследователи сообщают о достижении достаточно высоких результатов детектирования при применении той или иной комбинации ряда определяющих успех подобных экспериментов моментов, а именно, примененных: метода DM, набора базовых признаков, метода выделения существенных признаков, обучающего и тестового наборов и т.д. Однако, до сих пор в инженерном и пользовательском сообществах наблюдается ярко выраженный плюрализм мнений в отношении степени ценности реального вклада, который может привнести применение эвристических средств в целом и DM средств в частности в реально функционирующих антивирусных системах.

С объективной точки зрения, основным преимуществом подобных систем являются потенциально высокая скорость принятия решения, способность к обнаружению ранее неизвестного вредоносного кода, концептуально заложенная возможность переобучения систем подобного класса при появлении изменений в трендах развития malware. Перечисленные потенциальные преимущества, однако, сходят на нет при детальном рассмотрении показателей качества детектирования malware. Специфика обсуждаемой задачи такова, что они должны максимально приближаться к 100%-ному порогу. Любой факт пропуска вредоносной программы, а тем паче ложного срабатывания, может иметь крайне негативные последствия для защищаемого объекта функционирующей и используемой информационной инфраструктуры. В реальной жизни данная коллизия, как правило, разрешается за счет разумного компромисса: применяются как сигнатурной поиск для выявления заведомо вредоносных программ, так и эвристические средства для поиска их

новых образцов. При этом показатели качества последних не редко выверяются для недопущения ложных срабатываний любой ценой, что в итоге может повлиять на качество выявления объектов целевой категории.

Таким образом, одной из основных целей разработки методов эвристического поиска malware является повышение точности детектирования в условиях его высокой вариативности.

Одним из возможных вариантов оптимизации показателей предиктивной функции эвристических средств, основанных на методах DM, является применение комбинирования отдельных решающих экспертов (классификаторов). В данной работе этот вопрос рассматривается в контексте объединения отдельных существующих и доказавших свою потенциально высокую эффективность методов статического детектирования malware. Постановку решаемой задачи можно сформулировать следующим образом:

> *«Существует ряд существенно различающихся статических подходов к обнаружению malware, основанных на применении методов DM и доказавших свою потенциальную жизнеспособность. Каждый из них воплощает некоторую стратегию принятия решения, эффективность которой определяется как минимум используемым набором статических признаков и используемым классификатором. Насколько можно повысить общую точность принятия решения при формировании комбинации классификаторов? Какие из базовых методов комбинирования результатов работы классификаторов наиболее эффективны? Является ли эффективной стратегия комбинирования путем построения иерархической схемы принятия решения?»*

В настоящей работе представлены начальные результаты решения данной задачи при установке фокуса на использование различных типов статических признаков при анализе файлов формата PE32. Данные наборы признаков были выбраны по результатам исследования использования файлов PE32 и изучения ряда работ, посвященных тематике реализации статических методов детектирования malware на базе DM.

В качестве признаков для использования методов DM применяются следующие данные:

- данные, доступные из базовых заголовков, характеризующих структурные особенности анализируемого файла;
- данные секции импорта, представляющие базовый набор функций операционной системы, используемых приложением при функционировании;
- данные о наличии в исполняемых секциях анализируемого объекта тех или иных байтовых последовательностей (так называемых n-грамм);
- позиционно-зависимые данные, извлекаемые из ограниченного региона вблизи точки входа (Entry Point) в анализируемый файл.

Выделение из всего множества доступных признаков из указанных групп наиболее значимых производилось средствами критерия, основанного на вычислении коэффициента информационного усиления каждого признака, их приоритезации и извлечения ограниченного набора из верхней части полученного списка.

Для обучения отдельных решающих экспертов были применены методы классификации, продемонстрировавшие оптимальные показатели качества предиктивной функции в экспериментах, проведенных в работах по реализации статических методов детектирования malware на базе DM.: Naive Bayes и Decision Tree (C4.5).

Эксперименты по улучшению качества отдельных решающих элементов за счет применения методов комбинирования производились с использованием метода AdaBoost. Задача построения общего комбинированного классификатора решалась с использованием методов обобщения их конечных результатов: большинства голосов (Majority Vote), взвешенного большинства голосов (Weighted Majority Vote) и Байесовского комбинирования.

Проверка применимости стратегии комбинирования посредством построения иерархической схемы принятия решения производилась на основе очевидного тезиса, сводящегося к тому, что принятие решения о степени вредоносности программы должно проходить ряд этапов, очередность которых определяется практическими аспектами существующих процедур принятия решения. Известно, что статические методы детектирования malware менее эффективны в случае, когда исследуемый объект формата PE32 защищен средствами так называемых протекторов, обфускаторов, упаковщиков. Таким образом, представляется очевидным, что эффективность работы комбинированного классификатора существенно зависит от того, способен ли он на ранней стадии работы производить разделение файлов на отдельные группы, которые обладают теми или иными структурными особенностями. Для реализации первого уровня принятия решения в рассматриваемой иерархической схеме принятия решения использовался отдельный решающий элемент, работающий на классификаторе C4.5 и использующий позиционно-зависимые признаки. На втором уровне принятия решения использовался Байесовский принцип комбинирования классификаторов.

Для обучения классификаторов использовались файлы PE32, полученные с сайта VXHeavens, из системных каталогов операционной системы Windows XP. Инструментальная поддержка экспериментов осуществлялась средствами программного пакета Weka Classifier, собственными разработанными средствами парсинга файлов формата PE32 и форматирования исходных данных.

Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00826-а) и программы фундаментальных исследований ОНИТ РАН (проект № 3.2).