УДК 621.391.037

Е.О. Новаков, М.В. Цуранов

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

ИСПОЛЬЗОВАНИЕ ОБУЧАЕМЫХ HIPS-АНТИВИРУСОВ ДЛЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

В статье проведен анализ методов построения антивирусных систем. Указаны преимущества и недостатки основных методов защиты. Описаны виды HIPS антивирусов. Разработан алгоритм обучения HIPS-антивируса, устраняющий недостатки классических и экспертных реализаций антивируса. Описана программная модель предлагаемого антивирусного продукта.

Ключевые слова: *антивирусы, безопасность информации, проактивная защита, обучения антивирусов.*

Введение

В данный момент использование систем антивирусной защиты подвергается большой критике со стороны разработчиков. Основные претензии к антивирусам следующие: крупные антивирусные продукты (не считая встроенного в Windows) не обеспечивают повышение безопасности, а, скорее, вредят компьютерам. Как пример, можно посмотреть на список критических ошибок в антивирусном ПО, перечисленные в Project Zero компании Google [1]. Приведенные уязвимости показывают, что антиврусные продукты не только предоставляют множество способов для атак, но и в целом их разработчики не следуют стандартным правилам безопасности. Кроме этого, программный код всех сторонних антивирусов зачастую некорректно написан, и из-за этого разработчикам браузеров (и любого другого ПО прикладного уровня) сложнее следить за безопасностью своих продуктов [1].

Большинство разработчиков прикладного ПО при внедрении функции безопасности сталкиваются с противодействием со стороны антивирусных программ. Например, при внедрении технологии ASLR, используемую для изменения расположения в адресном пространстве процесса важных структур данных, в браузер Firefox для Windows. Тогда оказалось, что многие антивирусные программы мешают обновлению безопасности, интегрируя собственные библиотеки ASLR. Более того, несколько раз антивирусы даже заблокировали обновления Firefox, из-за чего пользователи не смогли получить важные исправления безопасности [1].

Однако, разработчики антивирусов реагируют на возникшие проблемы и активно внедряют приходят новые технологии антивирусостроения: Host-based Intrusion Prevention System (HIPS), Sandbox, Virtual-based Intrusion Prevention System (VIPS). Эти технологии позволяют пользователю активно мониторить процессы в системе и принимать решения о допуске их к различным функциям ОС.

Цель предложенной работы: разработка метода обучения HIPS-антивируса.

Изложение основного материала

Первые антивирусы использовали принцип реактивной защиты, которая была наиболее проста в реализации. Ее суть — обнаружение вторжения, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий [2]: удалить инфицированный файл; отправить файл в «карантин»; попытаться восстановить файл, удалив сам вирус из тела файла.

Классические реактивные системы обнаружения вредоносных программ, несмотря на кажущуюся простоту реализации и надежность, имеют ряд существенных недостатков [3]: слабая эффективность против угроз типа zero-day, так как эффективность напрямую связана с базой сигнатур вредоносного ПО, в которую внесены сигнатуры только известного, на данный момент, вредоносного ПО; необходимость постоянного обновления базы сигнатур вирусов для эффективной защиты от нового вредоносного ПО; для определения вредоносного ПО необходима процедура сканирования, которая отнимает достаточно много времени и системных ресурсов.

Указанные причины послужили толчком к развитию проактивных систем защиты. Основная причина — требование к постоянному пополнению базы сигнатур вирусов для реактивных методов, которые составляют большинство, на данный момент, ведь количество вирусов с каждым днем растет. Постоянно пополняющиеся базы сигнатур затрудняют поиск, что замедляет работу классических антивирусов, в то время как один вирус может иметь несколько сигнатур. К примеру, руководитель Comodo подверг критике стратегии антивирусной защиты [4]:

«Нельзя мириться с существованием отрасли, в которую вкладывается 10 миллиардов долларов без видимого результата. Давайте сравним. Допустим, вы платите три доллара за таблетки от головной боли, вы их принимаете, и боль проходит – ваша проблема

решена; и в то же время мы все платим индустрии безопасности 10 млад за решение проблем с вредоносным программным обеспечением, но оно не исчезает – напротив, его становится все больше и больше. Почему? Потому что нет корректной бизнес-модели».

В мае 2014 г. Брайан Дай (Brian Dye), старший вице-президент Symantec по информационной безопасности, рассказал газете Wall Street Journal, что классические антивирусы «обречены на неудачу». Он признался, что выпуск локальных решений для защиты персональных компьютеров «не прибыльный бизнес», и что компании необходимо это учитывать в своей стратегии. Представитель Symantec пояснил, что сегодня хакеры проводят атаки на компьютеры и вычислительные сети, а не занимаются рассылкой почтовых сообщений с зараженными вложениями. Хотя антивирусные продукты по-прежнему приносят Symantec весомую часть выручки (около 40%), компания не может добиться роста в этом сегменте [5].

Исходя из всего написанного, а также высказывания директора Comodo и перехода Symantec на полностью безсигнатурную работу, можно сделать вывод, что классический подход к обеспечению безопасности компьютера становится все менее актуальным и следует переходить к более современным проактивным методам защиты. Это позволит отойти от использования громоздких баз, поиск по которым потребляет все больше ресурсов ПК пользователя и увеличить надежность антивирусных систем против угроз zero-day. Примером такой проактивной системы защиты являются HIPS-антивирусы. Существуют следующие типы HIPS-систем: классические, экспертные, песочница. Классические HIPS-продукты предоставляют пользователю информацию об активности того или иного приложения, однако решение о разрешении/запрещении той или иной операции должен принимать пользователь, т.о. классические HIPS-продукты позволяют пользователю тонко настроить те или иные правила контроля, но создание правил требует высокой квалификации пользователя. Это системы, в инвентарь которых входит специальная таблица правил открытого вида. Она представляет собой перечень правил, согласно которым фиксируется неправомерное действие потенциально опасных процессов. Она формируется пользователем либо производителем продукта и может быть модифицирована. Ориентируясь на эту таблицу, драйверы HIPS могут автоматически запретить или разрешить какие-либо действия различных приложений, а также отправить пользователю запрос, чтобы он сам принял решение. Как следствие, для успешной работы классического HIPS пользователь должен обладать хоть какими-либо знаниями о системе, т.к. устройство, по сути, ориентировано на ручное управление, что является недостатком. Однако есть и достоинства: данную систему легче реализовывать, и она не требует значительных ресурсов для функционирования. Для примера подобного вида HIPS можно взять программы System Safety Monitor и AntiHook [6]. Экспертные HIPS способны проводить анализ активной работы запущенного приложения и оценивать его действия "в целом". Это значит, что если совокупность действий приложения схожа на разрушающую программу или на любое другое вредоносное действие - система сообщит пользователю о возможной опасности.

Поведенческие эвристики — это набор правил, которыми руководствуется программа для пометки процесса как «вредоносного» или нет в процессе его работы или запуска. Анализ проводится по таким параметрам как: память, к которой обращается процесс, драйвера, которые он запрашивает, влияние на другие процессы и прочие параметры, которые каждый HIPS реализует по-своему. В отличие от классических HIPS-продуктов, экспертные HIPS могут самостоятельно принимать решение о блокировке той или иной активности, исходя из правил и алгоритмов, заложенных разработчиком продукта. Для использования экспертных HIPS-продуктов пользователю не обязательно обладать определенной квалификацией. Экспертные HIPS-продукты в ряде случаев могут блокировать легитимную активность пользовательского программного обеспечения. Причинами этого могут быть: не идентификация данной активности программы как вредоносной из-за ошибок в алгоритме или коде программы, из-за неправильных настроек, либо идентификация безопасных процессов как опасных из-за особенностей их работы. Можно сказать, что качество экспертных HIPS зависит от того, насколько хорошо программа отличает опасные процессы от безопасных, ведь чем больше легитимных процессов блокируются, тем сложнее работать пользователю. Такие продукты основаны на черных и белых списках. Черный список (blacklist) — системы, суть работы которых заключается в проверке вхождения неизвестного файла, программы или действия в некий список заранее известных недоверенных объектов. Белый список (whitelist) — такие системы разрешают работу лишь программам из доверенного списка [6].

Следующий тип HIPS, песочница — специально выделенная среда для безопасного исполнения компьютерных программ. Обычно представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы — например, место на диске или в памяти. Доступ к сети, возможность связи с главной операционной системой или считывания информации с устройств ввода, обычно частично эмулируют, либо сильно ограничивают. Песочницы представляют собой пример виртуализации. Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников или «сырого» кода, который может случайно повредить систему или испортить сложную конфигурацию, как средство проактивной защиты от вредоносного кода, а также для обнаружения и анализа вредоносных, либо новых или недоверенных программ. Такие «тестировочные» песочницы копируют основные элементы среды, для которой пишется код, и позволяют разработчикам быстро и безболезненно экспериментировать с неотлаженным кодом.

В связи с большим распространением вредоносных программ, а также применением злоумышленниками специальных технологий (например, полиморфизм), классические сигнатурные сканеры уже не могут эффективно противостоять новым угрозам [6].

Основной недостаток HIPS систем: экспертных – ложные срабатывания, классических – потенциальная некомпетентность пользователя. Для устранения этих недостатков необходимо либо улучшить алгоритмы эвристики (для экспертных), что повлечет большие денежные и временные затраты, либо повышать компетентность пользователя, что тоже может привести к большим затратам. Однако, мы можем переложить формирование алгоритмов эвристики на опытного пользователя, с последующей передачей настроенной системы неопытному пользователю под конкретную сферу применение ПК пользователя антивируса. Это позволит сделать алгоритм эвристики более гибким, подстраивающимся под сферу использования системы защиты.

Исходя из этих пунктов, методика обучения антивируса состоит из таких пунктов:

1) формирование черного списка из базы данных антивируса или любого другого источника;

2) составление белого списка, добавлением в него ПО от доверенных разработчиков;

3) конструирование эвристических алгоритмов путем подключения модулей, каждый реагирует только на конкретное потенциально опасное поведение;

4) в случае, если процесс не был идентифицирован как опасный или безопасный, пользователь может принять решение: в какой список внести процесс.

Антивирусный продукт должен состоять из следующих модулей: UI (пользовательский интерфейс); Analyzer (блок перехвата процессов); Core (ядро системы). Блок «UI» представляет собой удобный пользовательский интерфейс с возможностью настройки модульного алгоритма эвристики, доступом к черному и белому спискам, списком заблокированных процессов с возможностью их разблокировать и всплывающего окна в случае, если был обнаружен неидентифицированный процесс. Блок «Analyzer» зависит от используемой ОС, так как осуществляет перехват процессов, что зависит от API конкретной системы и не может быть кроссплатформенным решением. Следовательно, этот блок должен быть реализован на native-code. Перехватив процесс, блок «Analyzer» передает сведения в блок «Core» для последующей обработки и выдачи автоматизированного решения, либо запроса к пользователю. Блок «Core» состоит из метода приведения процесса к понимаемому программой объекту, черного и белого списка, модулей алгоритма эвристики. Данный блок решает, будет ли процессу разрешен доступ в систему, основываясь на автоматизированной системе, либо ответе пользователя.

Выводы

Предлагаемая методика формирования модулей эвристики позволяет привлекать экспертов в своих областях для конкретных сфер применения продукта, в то же время, пользователю дана возможность формировать правила самостоятельно, если он уверен в своей компетентности. Это повышает гибкость системы, оставляя элементы автоматизированной работы. Модульность алгоритмов позволяет сосредоточиться на максимально опасных угрозах для каждой сферы или их совокупности, без затрат на обработку несущественных уязвимостей.

Список литературы

1. *Разработчик Firefox призвал пользователей Windows 10 отказаться от сторонних антивирусов [Электронный ресурс] – Режим доступа: https://4pda.ru/2017/1/31/334759/ 06.02.16*

2. *Обнаружение, основанное на сигнатурах [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/ 06.02.16.*

3. *Проактивные методы антивирусной защиты [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/blog/199/1300 06.02.16 .*

4. *Почему Comodo бесплатен? [Электронный ресурс] – Режим доступа: http://comodo.comss.ru/pochemu-comodo-besplaten.html 06.02.16.*

5. *Легендарный Norton Antivirus уходит с рынка [Электронный ресурс] Режим доступа: http://www.cnews.ru/news/top/legendarnyj_norton_antivirus_uhodit. 06.02.16.*

6. *HIPS [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/HIPS 06.02.16.*

Надійшла до редколегії 1.02.2017

Рецензент: д-р техн. наук, проф. О.А. Серков, Національний технічний університет «ХПІ», Харків.

ВИКОРИСТАННЯ НАВЧАЄМИХ HIPS-АНТИВІРУСІВ ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Є.О. Новаков, М.В. Цуранов

У статті приведений аналіз методів побудови антивірусних систем. Вказані переваги та недоліки основних методів захисту. Описані види HIPS-антивірусів. Розроблений алгоритм навчання HIPS-антивірусу, усуваючий недоліки класичних та експертних реалізацій антивірусу. Описана програмна модель пропонованого антивірусного продукту.

Ключові слова: *антивіруси, безпека інформації, HIPS, проактивний захист, навчання антивірусів.*

USING OF EDUCABLE HIPS-ANTIVIRUSES FOR CYBERCRIME OPPOSITION

Ye.O. Novakov, M.V. Tsuranov

The article has analysis of antivirus systems developing. Advantages and disadvantages of general security methods are listed. HIPS-antiviruses kinds are described. Teaching method which removes disadvantages of classical and expert antivirus implementations is designed in the article. Program model of the offered antivirus product is described.

Keywords*: antiviruses, information security, HIPS, proactive defense, antiviruses teaching.*