DARPA Active Authentication Program: Behavioral Biometrics также схожий по функционалу продукт. В 2013 году на RSA Conference Asia Pacific были представлены некоторые его концепты и результаты его тестирования. Также были приведены математические формулы расчета и анализа «доверия» анализируемому пользователю. Данный программный продукт опирается на большое количество разнообразных критериев оценки и поведенческих параметров. По результатам тестирования, программа может определить неверного пользователя в течении 10 секунд использования компьютера (6 взаимодействий, в среднем 3 нажатия клавиш) или же менее чем за 3,5 минут использования мыши [3].

SilentSense, мобильное приложение, считывающее действия пользователя за устройством и с высокой точностью определяющее, является ли он владельцем телефона. Считывая нажатия на экран, различные движения, и показания акселерометра, программа за 10 действий может определить валидность пользователя с вероятностью ошибки меньше 1%. К сожалению, данный программный продукт не подходит для персональных компьютеров, но использованные в нем математические функции для расчета вероятности и «доверия» к пользователю, лежащие в свободном доступе, могут прилично поспособствовать разработке системы идентификации [4].

Разрабатываемое нами приложение предназначено для идентификации пользователя на базе поведенческой биометрии. Оно наглядно показывает работоспособность системы идентификации пользователя на базе поведенческой биометрии, позволяет создать профиль пользователя с параметрами поведенческой биометрии и в дальнейшем использовать его для анализа.

ЛИТЕРАТУРА

1. Свободная энциклопедия – Википедия [Электронный ресурс] / Распространенные технологии биометрии - Режим доступа: https://en.wikipedia.org/wiki/ Biometrics#Adaptive_biometric_systems. Дата доступа: 10.09.15.
2. Интернет-портал Хакер [Электронный ресурс]/ Человека можно идентифицировать после 4-6 нажатий клавиш - Режим доступа: https://xakep.ru/2014/12/18/keyboard-id/ . Дата доступа: 12.09.15.
3. Официальный сайт RSA Conference [Электронный ресурс]/ DARPA Active Authentication Program - Режим доступа: http://www.rsaconference.com/. Дата доступа: 12.09.15.
4. Свободная энциклопедия - Cornell University Libriary [Электронный ресурс]/ SilentSense - Режим доступа: http://arxiv.org/pdf/1309.0073.pdf Дата доступа: 12.09.15.

УДК 004.492

АНАЛИЗ ПРИНЦИПОВ ВНЕДРЕНИЯ, НАЗНАЧЕНИЯ, УПРАВЛЕНИЯ ПРОГРАММНЫХ ЗАКЛАДОК. ХАРАКТЕРНЫЕ ПРИЗНАКИ И КЛАССИФИКАЦИЯ ПРОГРАММНЫХ ЗАКЛАДОК

А.Е. РАМАШКА
(Представлено: канд. техн. наук, доц. К.Я. РАХАНОВ)

Рассмотрена возможная классификация программных закладок по принципам внедрения, назначения и управления. Проанализированы характерные признаки программных закладок.

Программная закладка – это внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию (недокументированные возможности программного обеспечения) [1].

В настоящее время проблема программных закладок является актуальной и требует немедленного решения. Таким образом, возникает потребность в методах и программных продуктах, способных успешно противодействовать подобным угрозам. Современное предприятие представляет собой сложноорганизованную систему со своими управляющими органами и объектами информатизации. Поскольку любое современное рабочее место уже трудно представить без компьютера, которые практически всегда объединены в общую вычислительную сеть, необходимо полностью обезопасить их от возможных утечек секретных данных и конфиденциальной информации.

Как правило, многие крупные компания скрывают факт взлома и получения конфиденциальной информации злоумышленниками. Но даже без этой большой части всеобщей статистики, можно провести анализ известных кибер-атак, которые, к слову были произведены с помощью программных закладок.

Самым ярким примером действия программной закладки является военный конфликт в Персидском заливе. Тогда при проведении операции «Буря в пустыне» система ПВО Ирака оказалась заблоки-

рованной по неизвестной причине. Несмотря на отсутствие исчерпывающей информации, высказывалось предположение, что ЭВМ, входящие в состав комплекса технических средств системы ПВО, закупленные Ираком у Франции, содержали специальные управляемые «электронные закладки», блокировавшие работу вычислительной системы путем воздействия из вне защищаемого объекта [2].

Периодически эксперты обнаруживают недокументированных возможности в ПО для аппаратных комплексов. Например, в информационном бюллетене CERT CA-2002-32 объявлено о существовании программной закладки (backdoor) в операционной системе AOS (Alcatel Operating System) версии 5.1.1, применяемой для управления коммутаторами Alcatel OmniSwitch 7700/7800. Эта закладка запускает telnet-сервис на порту 6778/TCP, что может позволить удаленному злоумышленнику неавторизованно управлять коммутатором [3].

Есть случаи, когда уволенныые программисты похищали корпоративные данные через оставленный собой же «черный ход» (backdoor) в программе или нарушали работоспособность [4].

Присутствие программных закладок обнаруживается по следующим признакам:

1. Наличие в исходном коде исполняемого файла алгоритмического описания функций, назначение которых явно не декларировано разработчиком;
2. Изменение структуры исполняемого файла;
3. Изменение цифровой подписи исполняемого файла;
4. Обращение к области памяти другого процесса, изменение и уничтожение данных в области памяти другого процесса;
5. Обращение к внешним устройствам хранения информации и файловой системе в целом;
6. Инициализация сетевых подключений;
7. Аномальная сетевая активность;
8. Аномальное потребление аппаратных ресурсов.

Таким образом, можно выделить основные классификационные признаки программных закладок:

1. Метод внедрения: программные закладки могут внедряться на этапе разработки и при уже использовании готового продукта путем инъекций кода в исполняемые файлы либо обновления программного обеспечения до новой версии;
2. Назначение: программные закладки предназначаются для копирования, изменения, уничтожения конфиденциальной информации или внесение изменений в алгоритмы работы программного обеспечения. Так же возможен сценарий использования программных закладок для нарушения работоспособности информационных систем;
3. Метод управления: срабатывание программной закладки может быть привязано к какому либо событию в системе, в которую она внедрена, либо срабатывание может быть вызвано удаленно, если инициируются сетевые подключения.

На основании вышеперечисленных признаков, можно предложить классификацию программных закладок:

1. Классификация по методу внедрения:
1.1. Внедрение на этапе проектирования программного обеспечения;
1.2. Внедрение в готовое программное обеспечение.
2. Классификация по назначению:
2.1. Копирование конфиденциальной информации;
2.2. Изменение конфиденциальной информации;
2.3. Уничтожение конфиденциальной информации;
2.4. Изменение алгоритмов работы программного обеспечения;
2.5. Нарушение работоспособности системы в целом.
3. Классификация по методу управления:
3.1. Автоматическое срабатывание;
3.2. Удаленный вызов срабатывания.

Вывод. Используя предложенную классификацию и программных закладок, возможно создание эффективной системы борьбы с программными закладками и не декларированными возможностями программного обеспечения. Детальная классификация позволяет разработать точные алгоритмы для обнаружения и минимизации воздействия программных закладок.

ЛИТЕРАТУРА

1. Шабанов, И. Технологии и бизнес [Электронный ресурс] / И. Шабанов. – 2011. – Режим доступа: http://miratech.ua/sites/default/files/documents/press_about_us/pau20110427article1.pdf. – Дата доступа: 17.09.2015.

2. Лукашкин, К.А. Проблемы безопасности программного обеспечения военной техники [Электронный ресурс] / К.А. Лукашкин // Военное дело. – 2001. – Режим доступа: http://www.soldiering.ru/psychology/safe_soft_militaryequip.php. – Дата доступа: 17.09.2015.
3. Ian A. Finlay. Backdoor in Alcatel OmniSwitch AOS [Электронный ресурс] / Finlay // Carnegie Mellon University. – 2015. – Режим доступа: http://www.cert.org/historical/advisories/CA-2002-32.cfm. – Дата доступа: 20.09.2015.
4. Группа компаний InfoWatch [Электронный ресурс] / InfoWatch. – 2015. – Режим доступа: https://www.infowatch.ru/sites/default/files/files/products/appercut/Appercut_Company_Brochure_Rus.pdf. – Дата доступа: 16.09.2015.

УДК 004.42

ФУНКЦИОНАЛЬНАЯ СТРУКТУРА СИСТЕМЫ БОРЬБЫ С АНОМАЛЬНОЙ АКТИВНОСТЬЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

А.Е. РАМАШКА
(Представлено: канд. техн. наук, доц. К.Я. РАХАНОВ)

Рассмотрена возможная функциональная структура системы для борьбы с аномальной активностью программного обеспечения с применением облачных технологий.

В последнее время, в связи с ростом скорости внедрения информационных технологий в экономику и промышленность, наиболее остро встала проблема защиты конфиденциальных и секретных данных, представляющих определенную ценность, будь то определенные технологии производства или же данные о клиентах.

С точки зрения информационных технологий особую опасность представляют сами средства вычислительной техники в первую очередь компьютеризированные рабочие места сотрудников предприятия [1]. Одним из способов получения несанкционированного доступа к информации является внедрение в программное обеспечение не декларированных возможностей, которые порождают аномальную активность программного обеспечения.

Автоматизированная система должна представлять собой программный комплекс для выявления аномальной активности программного обеспечения, а также устранения возможности изменения информации и несанкционированного доступа к ней.

Система обнаружения аномальной активности должна удовлетворять следующим требованиям:

1) анализировать поведение исследуемого процесса (приложения);
2) возможность сигнатурного анализа исполняемого файла исследуемого процесса;
3) возможность анализа сетевых соединений, открываемых процессом;
4) возможность анализа сетевого трафика, генерируемого приложением;
5) реализация принятия решений оператором и в автоматическом режиме;
6) отвечать требованиям отказоустойчивости (сбой работы элемента системы, атаки на злоумышленников на ресурсы системы);
7) сохранение высокой производительности при пиковых нагрузках;
8) балансировка нагрузки между несколькими модулями обнаружения угроз;
9) низкая нагрузка на аппаратные мощности и ресурсы вычислительной машины;
10) поддержка облачных вычислений.

Исходя из вышеперечисленных требований система состоит из компонентов:

1) подсистема получения информации о сетевой активности приложений;
2) подсистема перехвата сетевых пакетов;
3) подсистема контроля целостности системы;
4) подсистема обнаружения угроз;
5) подсистема автоматического реагирования;
6) подсистема распределения нагрузки;
7) подсистема удаленного управления;
8) подсистема администрирования;
9) подсистема авторизации.

Подсистема получения информации о сетевой активности предназначена для постоянного мониторинга всех процессов на компьютере пользователя, а также получения данных о сетевых подключениях, инициированных этими процессами.

Подсистема перехвата сетевых пакетов предназначена для сбора данных о всех сетевых пакетах, генерируемых или получаемых процессами на компьютере пользователя.