РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО СЕВЕРО-ЗАПАДНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ (Управление Роскомнадзора по Северо-Западному федеральному округу)

ул. Галерная, д.27, Санкт-Петербург, 190000
тел.: (812) 5719566; факс (812) 5712731
E-mail: rsockanc78@rkn.gov.ru

_____ № _____

на № _____ от _____

СПбГУТ
Диссертационный совет Д 99.2.038.03

ОТЗЫВ

на автореферат **Шарикова Павла Ивановича** на тему: «Разработка стратифицированных методик создания и вложения устойчивого к атакам декомпиляцией и обфускацией цифрового водяного знака в байт-код class-файлов java-приложений и информационных систем», по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертационной работы.

Сильная распространенность информационных систем накладывает помимо очевидной пользы и эффективности накладывает дополнительные риски для пользовательских данных. Появляются новые способы, инструменты для незаконного получения пользовательских данных, проведения запрещенных транзакций, введения в заблуждение пользователей информационных систем.

Необходимо на постоянной основе осуществлять мониторинг состояния информационной системы, вовремя реагировать на любые внештатные изменения в ее структуре или компонентах. Необходимо отслеживать возможные утечки исходных файлов информационной системы с целью

предотвращения появления фишинговых сайтов с помощью которых осуществляется процедура фарминга.

Таким образом, диссертационная работа Шарикова Павла Ивановича является крайне актуальной так как цифровой водяной знак в исполняемых файлах способен решить ряд актуальных задач в сфере надзора.

Основные результаты, выносимые на защиту:

1. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе недекларированных возможностей виртуальной машины Java.
2. Методика создания и вложения цифрового водяного знака в class-файлы java-приложения устойчивого к атакам декомпиляцией направленных на его разрушение.
3. Методика создания и вложения цифрового водяного знака в class-файлы информационной системы устойчивого к атакам обфускацией направленных на его разрушение.

Научная новизна полученных результатов.

Научная новизна результатов заключается в том, что:

1. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе недекларированных возможностей виртуальной машины Java позволяет создать и произвести вложение цифрового водяного знака в class-файлы. Отличается от существующих тем, что позволяет вложить цифровой водяной знак большего объема.
2. Методика создания и вложения цифрового водяного знака в class-файлы java-приложения устойчивого к атакам декомпиляцией направленных на его разрушение позволяет создать и вложить цифровой водяной знак увеличенного объема и устойчивый к атакам декомпиляцией. Таким образом, скомпрометированные исполняемые файлы невозможно декомпилировать не нарушив логику работы.

3. Методика создания и вложения цифрового водяного знака в class-файлы информационной системы устойчивого к атакам обфускацией направленных на его разрушение позволяет создать и вложить единый цифровой водяной знак регистратор для всей информационной системы, который устойчив к атакам обфускацией. Данный цифровой водяной знак позволяет отслеживать изменения в информационной системе, а также ее целостность.

Теоретическая значимость результатов

Теоретическая значимость результатов заключается в развитии теории методик цифровой стеганографии в исполняемых файлах.

Практическая значимость результатов

Практическая значимость результатов заключается в:

1. Возможности использования цифрового водяного знака для отслеживания скомпрометированных файлов информационной системы и java-приложений посредством их проверки на наличие цифрового водяного знака.

2. Возможности контроля целостности информационной системы персональных данных посредством перманентной проверки неизменности цифрового водяного знака регистратора.

3. Возможности проверки фейковых сайтов и доказательства их незаконности при наличии заимствований кода и исполняемых файлов оригинальной информационной системы.

4. Невозможности полноценной декомпиляции скомпрометированных class-файлов java-приложений с целью получения исходного кода для дальнейшего осуществления процедуры фарминга.

5. Устойчивости цифрового водяного знака к атакам обфускацией при использовании инструмента оптимизации, как средства атаки для разрушения цифрового водяного знака и последующей компрометации исполняемых файлов без него.

Основные положения работы докладывались и обсуждались на 10 российских и международных конференциях.

Все результаты, выносимые на защиту, соответствуют п.п. 7 и 17 паспорта научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Недостатки работы

Судя по автореферату, к недостаткам можно отнести:

1. Не указано могут ли действия по созданию и вложению цифрового водяного знака исказить или уничтожить персональные данные в информационной системе.
2. Не указана возможность применения разработанных методик для информационных систем применяемых в анализе средств массовой информации.

Указанные замечания не влияют на общую положительную оценку диссертационной работы Шарикова П.И.

Выводы:

Диссертационная работа Шарикова П.И на тему «Разработка стратифицированных методик создания и вложения устойчивого к атакам декомпиляцией и обфускацией цифрового водяного знака в байт-код class-файлов java-приложений и информационных систем» является законченной научно-квалификационной работой, содержащей в себе решение научной задачи, теоретическую значимость, практическую значимость и научную новизну. Цель работы является актуальной.

Диссертационная работа соответствует всем требованиям п. 9 – 14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к кандидатским диссертациям, а ее автор, Шариков П.И., заслуживает

присвоения ученой степени кандидата технических наук по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность.

Отзыв составил:

Заместитель руководителя, Потехин И.Ю.

кандидат физико-математических наук

21.02.2024

Управление Роскомнадзора по Север-Западному федеральному округу

Почтовый адрес: ул. Галерная, д.27, Санкт-Петербург, 190098

Тел.: (812) 678-95-26.

e-mail: i.potehin@rkn.gov.ru