ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети и сетевые технологии: учебное пособие / П. П. Урбанович, Д. М. Романенко. – Минск: БГТУ, 2022. – 606 с.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ. – Минск: БГТУ, 2016. – 220 с.

3. Moyer F. What is end-to-end encryption?[Электронный ресурс]. – 2022. – Режим доступа: http://bp21.org.by/ru/art/a041031.html. – Дата доступа: 02.04.2023.

УДК 004.491.22

Студ. А.Д. Мозолевский, М.Л. Дащинский
Науч. рук. проф. П. П. Урбанович
(каф. информационных систем и технологий, БГТУ)

ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ И МОДЕЛИ ОБНАРУЖЕНИЯ ТРОЯНСКИХ ПРОГРАММ REMOTE ACCESS TROJAN

Троянские программы Remote Access Trojan (RAT) – это вид вредоносного ПО, который может получить удаленный доступ к зараженному устройству без согласия его владельца [1]. RAT-программы могут быть использованы для кражи личной информации, включая пароли, банковские данные и другие конфиденциальные данные [2]. Заражение троянской программой RAT может происходить по разным каналам. Одним из распространенных способов заражения RAT является установка программного обеспечения, содержащего в себе RAT.

Для обнаружения RAT существует несколько подходов. Один из наиболее распространенных – это сигнатурная модель [3]. Этот метод использует базу данных сигнатур, которые определяют уникальные характеристики RAT-программ. Поведенческая модель использует набор поведенческих характеристик, которые определяют вредоносное поведение RAT на зараженном устройстве: изменения файловой системы или сетевой активности могут указывать на наличие RAT-программы. Модель машинного обучения использует алгоритмы, которые могут обучаться на большом количестве данных, чтобы распознавать и обнаруживать RAT-программы на зараженных устройствах [4]. Аномальный метод обнаружения использует анализ необычных паттернов в данных. Например, если RAT-программа пытается изменить системные файлы, это может быть необычным событием, и метод аномального обнаружения может сработать.

В рамках исследования функциональных особенностей и моделей обнаружения троянских программ RAT была разработана упрощенная версия данного вредоносного ПО. Она имеет следующий функционал: просмотр содержимого директорий, скачивание файлов, шифрование/дешифрование файлов, удаленный вызов консольных команд. Возможность просмотра директории на зараженном компьютере позволяет злоумышленникам получить доступ к файлам и директориям, которые хранятся на компьютере пользователя.Скачивание файлов может привести к утечке информации пользователя.Функция шифрования/дешифрованияфайлов позволяет злоумышленникам зашифровать файлы на компьютере жертвы и требовать выкуп за расшифрование.Вызов консольных команд дает злоумышленникам возможность выполнять различные действия на зараженном компьютере, такие как установка программного обеспечения, удаление файлов или изменение настроек системы. Это может привести к серьезным последствиям, таким как потеря данных или нарушение работы системы.

В связи с этим разработка программы, которая является упрощенной версией RAT, подчеркивает необходимость защиты от данного типа вредоносных программ. Рассмотрим несколько методов защиты от RAT.

1. Установка и регулярное обновление антивирусных программ является одним из основных методов защиты от RAT. Антивирусные программы могут обнаруживать и блокировать попытки входа троянских программ в систему.

2. Файервол. Предназначен для контроля сетевого трафика, блокирования нежелательных соединений и обнаружения попыток проникновения в систему. Позволяет предотвратить подключение к системе удаленных устройств, которые могут содержать троянские программы.

3. Контроль доступа. Установка прав доступа для пользователей и групп может помочь в предотвращении распространения RAT в системе. Ограничение прав доступа на файлы и папки может помешать проникновению в систему троянской программы.

Не существует универсального метода защиты от RAT, так как злоумышленники постоянно разрабатывают новые методы атак. Однако, комбинация различных методов может помочь существенно повысить уровень защиты от RAT и других угроз информационной безопасности.

ЛИТЕРАТУРА

1. RAT (RemoteAccessTrojan) [Электронныйресурс]. URL: https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan. – Дата доступа: 29.04.2023.

2. Урбанович, П. П. Защитаинформации: конспект-лекция, ч.1 = Information Protection, Part 1: Introduction To The Subject Area. – Минск: БГТУ, 2019. – 52 с. https://elib.belstu.by/handle/123456789/29335

3. RATKing: новая кампания с троянами удаленного доступа [Электронный ресурс]. URL: https://habr.com/ru/companies/bizone/articles/508324/– Дата доступа: 29.04.2023.

4. Методы и технологии защиты от вредоносных программ [Электронный ресурс]. URL:https://encyclopedia.kaspersky.ru/ knowledge/malware-protection-methods-and-techniques/ – Дата доступа: 29.04.2023.

УДК [004.056+003.26] (075.8)

Студ. К.М. Гуменникова
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Web-приложения содержат конфиденциальную информации, поэтому необходимо регулярно проверять приложения на наличие угроз [1]. Наиболее распространённым угрозамиweb-приложений являются: SQL-инъекции, XSS (Cross-SiteScripting – межсайтовый скриптинг), CSRF (Cross-SiteRequestForgery) и прочие угрозы (незащищенные загрузки файлов, недостаточная проверка прав доступа, недостаточное шифрование, недостаточный контроль целостности). В таблицепредставленыраспространённые угрозы web-приложениям и методы по их устранению [1–3].

Таблица – Распространенные угрозы и методы по их устранению

Угроза	Методы устранения
XSS-атаки	1. Фильтрация ввода данных; 2. Экранирование символов; 3. Использование CSP; 4. Обновление исходного кода
SQL-инъекции	1. Использование параметризированных запросов; 2. Использование контроля доступа к БД с правами доступа; 3. Использование библиотек и фреймворков (Django, Laravel, RubyonRails, ASP.NETCore)
CSRF	1. Добавление одного или нескольких токенов; 2. Использование политики SOP; 3. Использование флагов; 4. Подтверждение действий от пользователя; 5. Использование библиотек и фреймворков