Хихол Е.А. Разработка системы сбора набора данных для анализа эксплойтов // Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 12(50) с. 106–109

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

РАЗРАБОТКА СИСТЕМЫ СБОРА НАБОРА ДАННЫХ ДЛЯ АНАЛИЗА ЭКСПЛОЙТОВ

Хихол Е.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: hiholl3@mail.ru

В данной статье исследуется использование специальных сред для изолированного исполнения программ («песочниц») с целью сбора набора данных для последующего анализа эксплойтов. Представлены основные компоненты «песочницы», проведен их сравнительный анализ, описано использование вызовов API Windows для фиксации поведения вредоносных программ, а также предложена архитектура системы сбора набора данных для анализа эксплойтов.

Ключевые слова: Информационная безопасность; анализ вредоносных программ; кибербезопасность; набор данных; изолированная среда; классификация вредоносных программ; эксплойт.

DEVELOPING A DATA COLLECTION SYSTEM FOR EXPLOIT ANALYSIS

Khikhol E.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: hiholl3@mail.ru

This paper examines the use of sandboxes to collect data for exploit analysis. The paper presents the main components of a sandbox, compares them, describes the use of Windows API calls to record malware behavior, and proposes an architecture for collecting data for exploit analysis.

Keywords: Information security; malware analysis; cyber security; dataset; sandbox environment; malware classification; exploit.

Введение.

Цель исследования заключается в разработке архитектуры системы сбора данных для анализа эксплойтов (т.е. компьютерных программ, использующих уязвимости в программном обеспечении). Система должна позволить собрать набор данных вызовов API в операционной системе Windows, выполненных эксплойтами, представленными в базе данных Exploit-DB[1]. Для этого она должна включать в себя систему сбора и обработки данных от Exploit-DB (в том числе компиляции эксплойтов), песочницу, позволяющую запускать вредоносные файлы, и систему сбора и обработки информации о поведении и структурных характеристиках вредоносного программного обеспечения (ПО) [3, 6].

С помощью песочниц можно безопасно запускать вредоносное ПО в условиях, имитирующих реальную рабочую среду. Они применяются для анализа файлов и сбора

[1] https://www.exploit-db.com/

детализированной информации о поведении и структурных характеристиках вредоносного ПО, таких как вызовы API вредоносного ПО, дамп памяти, сетевой трафик и т.д. Песочница состоит из двух ключевых частей. Первая часть — это управляющая машина, на которой осуществляется анализ вредоносного ПО, сохраняются результаты в базу данных, и предоставляется веб-интерфейс для пользователей. Второй компонент — это анализирующие машины, на которых исполняется вредоносное ПО. Эти машины могут быть как виртуальными, так и физическими. В исследовании проведен подробный сравнительный анализ различных типов песочниц, доступных на рынке. Исследование охватывает ключевые характеристики, такие как поддерживаемая операционная система (ОС), стоимость, функциональность и требуемый уровень навыков для её использования. Были проанализированы следующие песочницы: Cuckoo Sandbox[2], FireEye Malware Analysis, Any.Run, Joe Sandbox, Check Point SandBlast Threat Emulation, FortiSandbox, Triage, Anubis, Falcon Sandbox, Hybrid analysis, CAPE Sandbox. В результате проведенного анализа, основанного на ключевых критериях, для разработки системы сбора данных была выбрана песочница Cuckoo Sandbox. Эта песочница поддерживает широкий спектр операционных систем, таких как Windows, Linux и macOS, что позволяет проводить анализ вредоносных программ на различных платформах. Одним из значимых преимуществ является наличие бесплатной версии с базовыми функциями, что делает её доступной для исследователей и разработчиков. Кроме того, Cuckoo Sandbox предоставляет информацию по каждому анализируемому объекту, включая скриншоты рабочего стола виртуальной машины, на которой запускается вредоносное ПО. При этом Cuckoo Sandbox имеет широкие функциональные возможности: она поддерживает анализ различных типов файлов, включая исполняемые файлы, документы, скрипты и даже URL-адреса, что помогает визуально оценить поведение вредоносной программы [4].

Cuckoo Sandbox включает в себя программное обеспечение для централизованного управления, которое контролирует процесс запуска и анализа образцов. Каждый анализ проводится на новой виртуальной машине в изолированной среде. Данная песочница состоит из управляющей машины (хоста, на котором работает управляющее ПО) и нескольких гостевых машин (виртуальных машин для выполнения анализа). Хост запускает основной компонент песочницы, который контролирует весь процесс анализа, а гостевые машины — это изолированные среды, где безопасно выполняются и исследуются образцы вредоносного ПО.

Вредоносные программы, действующие в операционной системе Windows, для достижения своих целей активно взаимодействуют с системными службами, используя API Windows. Предполагая, что вредоносное ПО работает на компьютере под управлением операционной системы Windows, оно должно использовать системные службы операционной системы. Все запросы к этим службам (вызовы Windows API) формируют вредоносное поведение. Программа, работающая в среде Windows, использует API для доступа к функциям, предоставляемым операционной системой. Когда приложение выполняется в операционной системе, оно вызывает различные API для выполнения своих задач. Анализ вызовов API позволяет получить подробное представление о том, как вредоносное ПО взаимодействует с операционной системой и как оно использует её ресурсы для реализации

[2] https://github.com/cuckoosandbox

своих функций. Таким образом, подход, основанный на вызовах API, широко используется для динамического анализа вредоносных программ, показывая точность их поведения [1, 5, 7].

Предлагаемая архитектура системы сбора данных для анализа эксплойтов включает следующие компоненты: (1) подсистема сбора и обработки данных от Exploit-DB, включая подсистему сбора данных, подсистему предобработки исходных кодов эксплойтов и подсистему компиляции эксплойтов; (2) Cuckoo Sandbox, включая сервер и кластер виртуальных машин; (3) систему сбора и обработки данных при запуске эксплойтов, включая систему сбора журналов API и их обработки и представления в JSON формате для последующего анализа [2].

Получаемые наборы данных могут применяться в различных исследованиях по анализу вредоносного ПО.

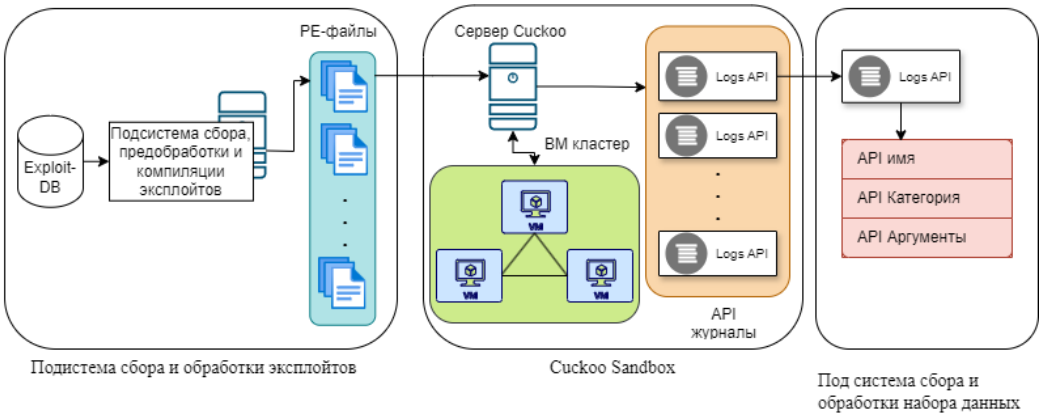

Рисунок 1. - Архитектура системы сбора набора данных для анализа эксплойтов

Заключение.

Основной целью было создание эффективной системы, которая может собирать, обрабатывать и анализировать данные о поведении вредоносных программ в безопасной и изолированной среде. Сбор данных о вызовах API имеет ключевое значение для понимания того, как вредоносное ПО использует ресурсы операционной системы для достижения своих целей. Через анализ этих вызовов можно выявить особенности поведения эксплойтов, которые не всегда очевидны при статическом анализе. Это делает подход, основанный на динамическом анализе с использованием вызовов API, критически важным для детального изучения методов эксплуатации уязвимостей. Важной частью системы является песочница, позволяющая безопасно исполнять вредоносное ПО. Cuckoo Sandbox обладает рядом преимуществ, таких как поддержка различных операционных систем, возможность анализа множества типов файлов и предоставление детализированной информации о поведении вредоносных программ. Эти возможности делают её идеальным кандидатом для целей данного исследования, так как она не только гибка и функциональна, но и доступна для широкого круга пользователей.

Список литературы

1. Ferhat Ozgur Catak, Cyber Security Institute Tubitak-Bilgem// 2021. A benchmark API call dataset for Windows PE malware classification. [Электронный ресурс] URL: 1905.01999.

2. Zhaoqi Zhang, Panpan Qi, Wei Wang. Dynamic Malware Analysis with Feature Engineering and Feature learning // School of Computing National University of Singapore. 2020. pp.1211-1212
3. Ferhat Ozgur Catak, Ahmet Faruk Yazi, Ogerta Elezaj and Javed Ahmed. Deep learning based Sequential model for malware analysis using Windows exe API Calls // PeerJ Computer Science. July 2020. pp.5-7.
4. **Cuckoo Sandbox Developers**. 2012. *Cuckoo Sandbox: Automated Malware Analysis*. URL: https://cuckoosandbox.org
5. Зайченко И.А., Большаков А.С. Об использовании системных вызовов WIN-API для обнаружения модифицированного вредоносного ПО // Телекоммуникации и информационные технологии. 2022. С. 28-36.
6. И. В. Гаврилов, Р. А. Смирнов. Предложения по реализации алгоритма автоматизации активного тестирования приложений. XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023)». 2. 2023. С. 513-518.
7. Я. А. Ильин, А. И. Катасонов. Определение характерных особенностей для обнаружения вредоносного программного обеспечения. XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2023)». 4. 2023. С. 629-633.

References

1. Ferhat Ozgur Catak, Cyber Security Institute Tubitak-Bilgem// 2021. A benchmark API call dataset for Windows PE malware classification. [Electronic resource] URL: 1905.01999.
2. Zhaoqi Zhang, Panpan Qi, Wei Wang. Dynamic Malware Analysis with Feature Engineering and Feature learning // School of Computing National University of Singapore. 2020. . pp.1211-1212
3. Ferhat Ozgur Catak, Ahmet Faruk Yazi, Ogerta Elezaj and Javed Ahmed. Deep learning based Sequential model for malware analysis using Windows exe API Calls // PeerJ Computer Science. July 2020. . pp.5-7.
4. Cuckoo Sandbox Developers. 2012. Cuckoo Sandbox: Automated Malware Analysis. URL: https://cuckoosandbox.org
5. Zaichenko I.A., Bolshakov A.S. On the use of WIN-API system calls to detect modified malware // Telecommunications and Information Technologies. 2022. pp. 28-36.
6. I.V.Gavrilov, R.A.Smirnov. Proposals for the implementation of an algorithm for automating active application testing. XII
7. A. Ilyin, A. I. Katasonov. Identify features for malware detection. XII International Scientific, Technical and Scientific-Methodological Conference "Actual Problems of Infotelecommunications in Science and Education (APINO-2023)". 4. 2023. pp. 629-633.