**УДК 004**

***Глухов Сергей Евгеньевич***
***студент 3 курса бакалавриата,***
***Математический факультет,***
***Ярославский государственный университет им. П.Г. Демидова,***
***Россия, г. Ярославль***
***e-mail: sergeyglukhov99@gmail.com***

# ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ПЕСОЧНИЦ В УЛУЧШЕНИИ БЕЗОПАСНОСТИ СЕТИ

***Аннотация:*** *В статье рассмотрены современные кибератаки. Рассказывается о технологии песочниц для улучшения безопасности сети. Выделены основные модели изоляции на основе технологии песочниц.*

**Ключевые слова:** технология песочниц, безопасность сети, изоляция, программное средство.

***Glukhov Sergey Evgenyevich***
***3rd year bachelor student,***
***Faculty of Mathematics,***
***Yaroslavl State University of P.G. Demidov,***
***Russia, Yaroslavl***

# USING SANDBOX TECHNOLOGY TO IMPROVE NETWORK SECURITY

***Abstract:*** *The article deals with modern cyberattacks. It describes the technology of sandboxes to improve network security. The main models of isolation based on sandbox technology are highlighted.*

**Keywords:** sandbox technology, network security, isolation, software.

Часто при проведении кибератак, преступники используют вредоносные программы, которые только появились и для которых еще не разработаны защитные механизмы. Они разрабатываются специально для определенных атак. Их называют угрозой “нулевого дня”. Порой они не заметны даже для самых современных специализированных программ обнаружения компьютерных вирусов.

Идентификацию таких угроз можно решить использованием технологии песочницы — это механизм безопасности, предназначенный для выполнения подозрительных программ в защищенной среде без риска нанести вред. К

песочницам относят виртуализованные среды, которые часто тем или иным образом эмулируют сетевые службы, обеспечивая нормальную работу исследуемого ПО [1].

Используя технологию песочниц, нет необходимости, например, предоставлять доступ в сеть или к внешним накопителям. Эти функции можно эмулировать. Таким образом можно защитится от атак, которые не идентифицируются самыми известными антивирусами.

Выделяют три основные модели изоляции на основе песочницы [2]:

1. Полная виртуализации. Использование виртуальной машины. Она служит защитным слоем между операционной системой и вредоносными программами. Недостатком является большой размер виртуальной машины и специализированных конфигураций. А также сложный обмен данными между системами.

2. Частичная виртуализации файловой системы и реестра. Позволяет предоставлять песочнице копии необходимых объектов файловой системы. При попытке изменения данных в этих объектах, будут модифицироваться только сами копии внутри песочницы

3. Изоляция на основе правил. Файловая система и реестр не виртуализируется. Составляется набор правил, осуществляющий внутреннюю защиту. Только точный набор таких правил, поможет защитится от заражения основной системы.

Одним из таких программных средств является песочница, от «Лаборатории Касперского». Она предоставляется в качестве одной из составляющей для анализа вредоносной активности. А также для создания и исследования антивирусных баз. Эта песочница является компонентом Kaspersky Anti Targeted Attack (KATA), платформы для защиты от целенаправленных атак, портала Kaspersky Threat Intelligence (KL TIP). Она позволяет классифицировать файлы и URL-адреса на вредоносные и безопасные. Также данная песочница может получать полезные и практичные сведения об

активности вирусных программ, для разработки более устойчивых и сложных алгоритмов обнаружения.

Принцип работы песочницы KATA, это аппаратная виртуализация. Она обеспечивает стабильность, прирост скорости и эффективности работы.

В настоящее время существуют виртуальные машины для платформ Windows и Android. а в планах на 2021 год — Linux. Помимо объектов и файлов операционных систем Windows и Android, песочница может анализировать URL-адреса. Она переходит по URL-адресу, обнаруживает загрузочные файлы, выявляет события JavaScript, исполнение Adobe Flash и др.

В рассматриваемой нами песочнице, создаются виртуальные образы операционных систем с уже предустановленными программами. В них она запускает объекты и анализирует их поведение для обнаружения вредоносных процессов. Результатами работы такой эмуляции являются: дерево угроз и опасной активности в изолированной среде или сети, доступное в JSON-формате, фиксирующие снимки операционной системы во время исполнения объектов и сам вредоносный предмет в зашифрованном и изолированном виде.

Технологии песочниц в настоящее время широко распространены. Они бывают довольно разнообразны, но преследуют одну цель — защитить сеть и конечные точки от атак, которые невозможно распознать традиционными методами. Это важная часть корпоративной системы информационной безопасности, без которой нельзя быть уверенным в 100% защите инфраструктуры.

**Список литературы:**

1. Сикорски М., Хониг Э., Вскрытие покажет. Практический анализ вредоносного ПО. СПб: Питер, 2018. 768 с.

2. Антивирусные песочницы. // Введение. [Электронный ресурс]. Режим доступа: URL: https://habrahabr.ru/post/105581/ (дата обращения: 10.01.2021 г.).