БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 3 (110). – 40–53

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004 DOI: 10.17212/2782-2230-2023-3-40-53

ВЫБОР И ОЦЕНКА ФУНКЦИОНАЛЬНОСТИ ЗАМКНУТЫХ СРЕД ВЫПОЛНЕНИЯ ПРОГРАММ («ПЕСОЧНИЦ») ДЛЯ ТЕСТИРОВАНИЯ И ДЕТЕКТИРОВАНИЯ ПОТЕНЦИАЛЬНО ОПАСНЫХ ФАЙЛОВ И ПРОГРАММ*

А.Б. АРХИПОВА[1], А.С. БЕРЕЖНОЙ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, доцент кафедры защиты информации. E-mail: arhipova@corp.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, инженер кафедры защиты информации. E-mail: kaf_zi@corp.nstu.ru*

Технологии «песочниц» предоставляют самые эффективные механизмы по защите от целевых атак и атак с использованием уязвимостей нулевого дня. Принцип работы «песочницы» заключается в том, что подозрительное программное обеспечение запускается в специально подготовленной для него среде, изолированной от остальной инфраструктуры. В работе выполнен анализ методов реализации «песочниц» для оценки и выбора функционала замкнутых сред. Рассмотрены локальные «песочницы», которые входят в состав многих антивирусов. Они обеспечивают изоляцию на базе частичной виртуализации файловой системы и реестра. Проанализированы сетевые «песочницы», которые имеют меньше ограничений, чем локальные, так как не снижают производительности компьютера пользователя и позволяют проверять потенциальные угрозы на различных операционных системах. Для выбора и оценки замкнутых сред в работе были выбраны две компании, которые предоставляют «песочницы» как в программно-аппаратном виде, так и с использованием готовых образов для сред виртуализации: FortiSandBox от компании Fortinet и PT Sandbox от компании Positive Technologies. Тестирование продуктов происходило в деморежиме, в виртуальной среде VMware workstation.

Ключевые слова: информационная безопасность, замкнутая среда, «песочница», тестирование продуктов, виртуализация, контейнеризация, функциональные возможности, гипервизор

* Статья получена 10 июня 2023 г.

ВВЕДЕНИЕ

При проведении целевых атак киберпреступники зачастую используют так называемые угрозы нулевого дня. Это вредоносные программы и эксплойты, которые только появились или были написаны специально для конкретной атаки и еще не попали в сигнатурные базы традиционных средств защиты. Подобные инструменты порой незаметны даже для наиболее современных антивирусов, межсетевых экранов и систем предотвращения вторжений. Решить задачу идентификации ранее неизвестных образцов вредоносных программ помогают сетевые или локальные «песочницы» – системы защиты, позволяющие оценить безопасность программного обеспечения путем его запуска и анализа в изолированном виртуальном окружении. Вместо применения сигнатурных методов поиска вредоносной активности «песочница» анализирует действия программы в среде, имитирующей типовые автоматизированные рабочие места и серверы организации. Стоит отметить, что правильная защита должна быть многослойной, и поэтому представители класса сетевых «песочниц» отнюдь не пренебрегают интеграцией с антивирусами, системами предотвращения вторжений и другими традиционными сигнатурными средствами.

1. ПОНЯТИЕ И МЕТОДЫ РЕАЛИЗАЦИИ «ПЕСОЧНИЦЫ»

Под «песочницей» (англ. sandbox) понимают ограниченную среду в компьютерной системе, предназначенную для исполнения потенциально опасных программ без их доступа к системным объектам операционной системы и иных приложений. «Песочницы» часто используют для запуска непротестированного кода, непроверенного кода из неизвестных источников, а также для запуска и обнаружения вирусов.

Технологии «песочниц» предоставляют самые эффективные механизмы по защите от целевых атак и атак с использованием уязвимостей нулевого дня. Принцип работы «песочницы» заключается в том, что подозрительное программное обеспечение (ПО) запускается в специально подготовленной для него среде, изолированной от остальной инфраструктуры. Известный и заведомо вредоносный код не попадает в «песочницу», поскольку он блокируется на уровне межсетевого экрана или сигнатурного анализа. А вот если у этих средств не набирается достаточного объема данных для принятия решения, файл направляется в «песочницу» [2].

Использование изолированных виртуальных машин для выполнения проверяемых объектов и эмуляция взаимодействия с пользователем позволяют подробно отследить характер выполняемых действий потенциально небез-

опасного ПО и решить, можно ли возвращать объект пользователю для запуска на рабочей станции. Интеграция анализа в «песочнице» с сигнатурным анализом и другими способами проверки в стандартных продуктах безопасности позволяет повысить эффективность выявления потенциальных угроз и улучшить от целевых атак.

Существуют различные типы «песочниц».

1. Локальные «песочницы». Входят в состав многих антивирусов. Они реализуют изоляцию на базе частичной виртуализации файловой системы и реестра. Вместо того чтобы создавать для каждого проверяемого процесса отдельную виртуальную машину, локальная «песочница» создает для них дубликаты объектов файловой системы и реестра [2]. Получается безопасная среда-«песочница» на компьютере пользователя. Если процесс изменит файлы или запишет что-то в реестр, изменятся лишь копии внутри песочницы, а реальные объекты не будут затронуты.

Изоляция файлов от основной системы обеспечивается с помощью контроля прав пользователей. Достоинством такого подхода является относительная простота реализации и невысокие затраты системных ресурсов. А в качестве недостатков можно отметить необходимость постоянной очистки контейнеров виртуализации для запуска каждого проверяемого файла.

Помимо этого, встречаются обходы такой реализации «песочницы», которые позволяют вредоносному коду перейти в основную систему [3].

Более защищенный вариант локальной «песочницы» предполагает создание отдельной виртуальной машины, копирующей рабочее окружение. Но затраты ресурсов на такой вариант, как правило, оказываются неприемлемо высокими, поэтому вместо него используются сетевые «песочницы», которые располагаются на выделенном сервере внутри сети компании или в облаке производителя антивирусного решения [4].

2. Сетевые «песочницы». Имеют меньше ограничений, чем локальные: они не снижают производительность компьютера пользователя и позволяют проверять потенциальные угрозы на различных операционных системах (ОС). Таким образом, система полностью изолирована от рабочего компьютера пользователя [5]. При необходимости такие «песочницы» могут эмулировать подключение к Интернету и работу со съемными носителями. При работе с сетевыми «песочницами» на компьютерах пользователей устанавливается агент – служба, которая отправляет попавшие под подозрения файлы в сетевую «песочницу». Передача файлов на анализ в облако занимает больше времени, чем при взаимодействии с сервером в сети компании.

В совокупности с длительностью анализа время ожидания результата может составить несколько минут, на протяжении которых запуск приложения будет «поставлен на паузу» до получения разрешения от «песочницы». В связи

с этим разработчики «песочниц» указывают максимальное время ожидания в SLA [6].

Вредоносное ПО, ориентированное на конкретную компанию, как правило, проверяет окружение, в котором оно запущено. И даже если ПО не содержит проверку на запуск в «песочнице», несоответствие окружения может привести к тому, что полезная нагрузка во время анализа не сработает и файл будет считаться безопасным. Чтобы избежать такой ситуации, нужно, чтобы рабочая среда, которую эмулирует «песочница», максимально точно соответствовала рабочим станциям реальных пользователей [7].

В случае с облачными «песочницами» добиться такого соответствия сложнее, в то время как загрузка образа рабочей станции на сервер компании не составляет сложности. Главное, чтобы выбранный вариант сервера-«песочницы» поддерживал работу с пользовательскими образами. Другими словами, чтобы максимально приблизить конфигурацию виртуальных машин внутри «песочницы» к корпоративной среде, нужно иметь возможность тонко настраивать их содержимое: изменять настройки операционной системы, редактировать перечень установленных языков, драйверов периферийных устройств, устанавливать дополнительный либо нестандартный софт и даже управлять содержимым рабочего стола, поскольку всё это и многое другое может расцениваться киберзлоумышленниками как условие для запуска либо незапуска вредоносных инструкций. Использование же стандартизированных образов для разворачивания виртуальных машин внутри «песочниц» легко отслеживается и позволяет применить механизмы обхода детектирования в «песочницах». «Песочницы» поддерживают возможность загрузки пользовательских образов вычислительных машин, что на практике неоднократно показывало более высокую эффективность при обнаружении вредоносного ПО в сравнении с «песочницами» производителей, использующих стандартизированные образы ВМ для анализа.

Анализ литературы показал, что исходя из соображений необходимости обеспечения максимальной эффективности на сегодняшний день предпочтение следует отдать сетевому варианту. Реализации облачных «песочниц» на сегодняшний день ни у одного из производителей не поддерживают в качестве среды тестирования пользовательских образов виртуальных машин, точно отражающих инфраструктуру конкретного заказчика [8]. Облачные же «песочницы» могут рассматриваться в качестве более доступной по стоимости альтернативы либо если инфраструктура компании территориально распределена. В этом случае затраты на обеспечение необходимой сетевой маршрутизации могут превысить выгоду от разницы между облачным и серверным решением компании.

2. ВЫБОР И ОЦЕНКА ЗАМКНУТЫХ СРЕД

Для выбора и оценки замкнутых сред были выбраны две компании, которые предоставляют «песочницы» как в программно-аппаратном виде, так и с использованием готовых образов для сред виртуализации: FortiSandBox от компании Fortinet и PT Sandbox от компании Positive Technologies. Тестирование продуктов происходило в деморежиме, в виртуальной среде VMware workstation.

1. FortiSandbox – это замкнутая среда от Fortinet, предназначенная для обнаружения потенциально сложных атак в «песочнице». Она осуществляет анализ и выявление потенциально опасных угроз в локальной сети компании с эмуляцией кода в виртуальной защищенной среде. Песочница FortiSandbox, является как программно-аппаратным комплексом FortiSandBox 1000D/3000E/3500D, виртуальным устройством (FortiSandbox-VM), так и облачным решением с интегрированным межсетевым экраном FortiGate (FortiSandBox Cloud). FortiSandbox обеспечивает детонацию угроз, обнаружение и минимизацию последствий атак.

Для развертывания «песочницы» есть несколько подходов. В самом простом изолированном режиме «песочница» подключается к SPAN-порту коммутатора. Такое подключение лучше всего подходит для защиты от сложных угроз к уже имеющимся видам защиты. При таком подходе есть возможность загружать подозрительные файлы на проверку с помощью веб интерфейса. В продвинутом режиме внедрения возможно перехватывать или передавать контент для анализа из других продуктов компании Fortinet в FortiSandbox. Данный метод является наиболее эффективным, чтобы своевременно блокировать известные атаки без потери в производительности сети и обеспечивать мгновенное восстановление и генерацию отчетов от этих устройств. Есть возможность настроить оповещение о блокировке атак или о генерации отчетов через электронную почту.

Функциональные возможности FortiSandbox

В FortiSandbox используется метод эмуляции кода для раскрытия поведения и обнаружения неизвестных угроз и целенаправленных атак. Для оценки угроз исполняемых файлов, zip-архивов и других файловых расширений используется виртуальная среда, которая виртуализирует рабочую среду ОС и программное обеспечение. FortiSandbox имеет поддержку создания собственных образов, в которых может быть определенный набор программ, используемых заказчиком.

Анализ файла, который передается в изолированную среду, – затратный процесс как по времени, так и по ресурсам системы, что может значительно

снизить производительность и ограничить число проверенных файлов. Для оптимизации это процесса подозрительные файлы проходят предварительную фильтрацию: происходит процесс антивирусного сканирования и сравнения сигнатур файлов с базой. Если в ходе первой проверки антивирусным сканером не было подтверждено наличие или отсутствие угрозы в файле, то образец передается для дальнейшего анализа в «песочницу». В случае когда файл оказывается вредоносным, то «песочница» загружает данные о найденных угрозах в отчет, содержащий сведения о перехваченных пакетах, логах, трассировке, самих файлах и скриншотах.

Начальный доступ для настройки осуществляется с помощью средств ssh или com-порта для программно-аппаратного комплекса. В таком режиме выполняется только начальная настройка системы, поскольку настройка всего функционала происходит внутри графического интерфейса.

Список файлов, поддерживаемых по умолчанию в FortiSandbox, представлен в табл. 1 [20].

Таблица 1

Table 1

Поддержка файлов для анализа FortiSandbox

File support for analysis FortiSandbox

Тип файла	Расширения
Исполняемые	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF и VBS. Поскольку не все DLL-файлы могут быть выполнены в пределах виртуальной машины, рекомендуется для этого типа файлов включить предварительную фильтрацию
Архивные	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ и т. д.
Скриптовые	JavaScript/HTML, Batch Script, Power Shell, VBS
Microsoft Office	Word, Excel, PowerPoint, Outlook и т. д.
Adobe	PDF, SWF, Flash
Статические веб-файлы	HTML, JS, URL, LNK
Файлы ОС Android	APK

Повышение производительности и минимизация ложных срабатываний достигается за счет использования белого и черного списков. Эти списки хранят хеш, контрольные суммы, а также список демонов, с которых загружаются файлы.

Отметим, что сетевое устройство безопасности FortiSandbox является полнофункциональной сетевой «песочницей», интегрированной с анализом угроз и механизмами безопасности продуктов Fortinet, таких как FortiGate, что позволяет в режиме реального времени обеспечить безопасность контролируемой сети и конечных точек на каждом уровне защиты.

Физические устройства FortiSandbox предназначены для защиты вычислительных сетей крупных компаний и корпораций. Благодаря различным вариантам встраивания устройства могут распределять нагрузку и защищать удаленные сегменты сети. Использование таких устройств обусловлено их высокой производительностью. Однако использование дополнительных функций безопасности влечет за собой увеличение себестоимости решения. Для небольших компаний Fortinet предлагает альтернативный вариант сетевой «песочницы» без снижения скорости обнаружения и реагирования на угрозы безопасности – FortiSandbox Cloud.

Достоинства FortiSandbox:

- высокая производительность и скорость анализа сетевого трафика;
- наличие большого числа сетевых портов и возможность расширения за счет дополнительных интерфейсов;
- поддержка нескольких сценариев развертывания;
- интеграция с другими продуктами Fortinet;
- поддержка масштабируемости и кластеризации;
- Microsoft Office (только для WINXPVM и WIN7X86VM);
- управление единым средством централизованного управления FortiSandbox через веб-интерфейс.

Недостатки FortiSandbox:

- отсутствие русской локализации;
- использование дополнительных функций безопасности и образов виртуальных машин требует приобретение дополнительных лицензий.

2. PT Sandbox. «Песочница» PT Sandbox от компании Positive Technologies, имеет возможность гибко настраивать виртуальные среды так, чтобы они не отличались от реальных рабочих станций с ОС. Есть возможность загружать в них помимо стандартного офисного пакета программ тот или иной пакет специализированного ПО, используемого в организации. Эта особенность наряду с глубоким комплексным анализом файлов позволяет продукту обеспечивать защиту от целевых и массовых атак, сопровождающихся вредоносными программами и угрозами нулевого дня.

Замкнутая среда PT Sandbox анализирует объекты, которые попадают в инфраструктуру компании из разных источников, а именно: по электронной почте, скачиваются из сети, размещаются в корпоративных файловых хранилищах или загружаются пользователями через веб-интерфейс продукта.

Любой файл, отправленный в «песочницу», проходит комплексную проверку, которая включает в себя статистический и поведенческий анализ. По ее результатам формируется итоговый отчет. Статистический анализ предусматривает антивирусную проверку и анализ файла с помощью уникальных экспертных правил.

Для поиска уже известных вредоносных программ используется несколько антивирусов, которые поставляются вместе с продуктом. Поведенческий анализ предусматривает запуск файла в виртуальной среде и глубокое изучение его действий. Продукт не только анализирует сам файл и связанные с ним артефакты, но и проверяет генерируемый им трафик, выявляя вредоносную сетевую активность.

Функциональные возможности PT Sandbox

Продукт имеет возможность использовать два типа режима для анализа объекта: пассивный и блокирующий. В зависимости от типа анализа PT Sandbox будет или блокировать опасные файлы и письма, или отслеживать их. В пассивном режиме файлы и письма отправляются на проверку одновременно с их дальнейшей передачей. Все дальнейшие решения о распространении файла и их реализации на возникающие угрозы принимают операторы безопасности по результатам анализа.

В блокирующем режиме на время проверки продукт останавливает дальнейшую передачу файла или письма до получения результата. Если в задании на проверку выявлен хотя бы один опасный файл, то блокируются все файлы из этого задания. В этом режиме могут работать следующие источники: палка-шлюз, почтовый сервер с установленным агентом и почтовый сервер в режиме фильтрации.

Выявленные особенности «песочницы» после изучения функциональности и документации по продукту заключаются в следующем.

1. Обнаружение целевых атак (в том числе и атаки нулевого дня) на конкретное ПО. Продукт поддерживает глубокую настройку виртуализации для анализа и загрузки в них того ПО, которое реально используется в компании и может быть мишенью для злоумышленников.

2. Выявление угроз в сетевом трафике, включая шифрованный. Продукт анализирует весь трафик, который генерируется в процессе анализа файла, в том числе скрытый под TLS. Это дает возможность выявлять опасную сетевую активность, которая внешне может быть не связана с конкретным файлом.

3. Выявление скрытых в инфраструктурах ранее неизвестных угроз. Этого удается достичь с помощью регулярного ретроспективного анализа. После обновления баз знаний продукт выполняет автоматическую перепроверку уже обработанных файлов и находит угрозы, которые не детектировались на момент предыдущего исследования. Взаимодействие с продуктом происходит через веб-интерфейс, который делится на главное меню, расположенное в верхней части страницы, и рабочую область.

При работе PT Sandbox уделяется особое внимание качеству детектирования угроз. Помимо стандартной настройки для «песочниц» функциональности по анализу файлов, в продукте реализована возможность настройки виртуальных сред, проверка генерируемого файлом сетевого трафика (в том числе шифрованного) и автоматический ретроспективный анализ.

PT Sandbox позволяет осуществлять проверку сжатых файлов и архивов. По умолчанию декомпрессия перед проверкой отключена (табл. 2).

Таблица 2

Table 2

Поддерживаемые методы сжатия файлов PT Sandbox

Supported PT Sandbox File Compression Methods

Вид компрессии	Расширения
Gzip	.gz
Compress	.z
Bzip2	.bz2
LZMA	.lz, .lzma
LZMA2	.xz

Достоинства PT Sandbox:

- большое число источников файлов и писем для проверки (почтовые серверы, ICAP-сервер, папки-шлюзы, общие папки и др.), включая проверку по требованию пользователя через веб-интерфейс и с помощью почтовой службы;
- комплексная проверка файлов, сочетающая в себе статический и динамический виды анализа и обеспечивающая высокий уровень детектирования благодаря уникальным правилам PT ESC;

- поддержка анализа сетевого трафика и наличие ретроспективного анализа;
- подробный обзор действий файла, связанных с ним артефактов и сетевой активности, детальная визуализация операций в виртуальной среде (граф, видеозапись);
- удобный графический интерфейс для мониторинга и настройки заданий на проверку;
- интеграция с продуктами Positive Technologies и антивирусными средствами сторонних производителей;
- поддержка горизонтального масштабирования.

После анализа двух «песочниц» от разных компаний можно сказать, что «песочницы» отличаются незначительно, так как основные функции реализованы единообразно.

ЗАКЛЮЧЕНИЕ

Мировой рынок традиционно представлен большим числом крупных производителей, предлагающих продукты разного уровня – как по стоимости, так и по качеству защиты. Выбор конкретного решения существенно зависит от того, какие средства уже используются в инфраструктуре. Так, например, если в ней установлены продукты Check Point, Fortinet, Palo Alto или McAfee, то весьма логичным будет внедрение «песочницы», FortiSandbox. Это обеспечит бесшовную интеграцию продуктов. Если же целью является построение платформенно независимого комплекса, то, возможно, имеет смысл присмотреться к предложениям Positive Technologies. Учитывая ниспадающий объем целенаправленных атак на инфраструктуры организаций, можно утверждать, что сетевые «песочницы» актуальны для отечественного заказчика, и дальнейший спрос на них будет только расти. Это, несомненно, должно положительно сказаться на развитии российского рынка таких продуктов.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 56938–2016. Защита информации при использовании технологий виртуализации: введ. 2017–06–01. – М.: Изд-во стандартов, 2017. – 30 с.

2. Песочница (Sandbox) / Лаборатория Касперского. – URL: https://www.kaspersky.ru/enterprise-security/wiki-section/products/sandbox (дата обращения: 01.09.2023).

3. *Казыханов А.А., Попов К.Г.* Анализ использования песочниц для работы с зловредами // Символ науки. – 2016. – № 7-2. – С. 63–64.

4. Что такое песочница? Как работает облачная песочница? – URL: https://www.avast.ru/business/resources/what-is-sandboxing#pc (дата обращения: 04.09.2023).

5. *Солопов М.И., Чиркин Е.С.* Анализ степени изолированности защищенных сред средств обеспечения информационной безопасности // Гаудеамус. – 2012. – № 20. – С. 157–159.

6. Red Hat Enterprise Virtualization. Обзор продукта / Бюро Соломатина. – М., 2010. – URL: http://www.pcweek.ru/upload/iblock/eba/bureausolomatina-4.pdf (дата обращения: 04.09.2023).

7. *Баранов А.В., Николаев Д.С.* Использование контейнерной виртуализации в организации высокопроизводительных вычислений // Программные системы: теория и приложения. – 2016. – № 1 (28). – С. 117–134.

8. *Метельков А.Н.* Моделирование сценариев кибератак в киберполигонах // Вестник Санкт-Петербургского университета ГПС МЧС России. – 2023. – № 2. – С. 161–176.

9. *Метельков А.Н.* Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. – 2022. – № 1. – С. 51–60.

10. The current state of the art and future of European cyber range ecosystem / C. Virág, J. Cegan, T. Lieskovan, M. Merialdo // 2021 IEEE International Conference on Cyber Security and Resilience (CSR). – Rhodes, Greece, 2021. – P. 390–395.

11. *Davies J., Margat S.* A survey of cyber ranges and testbeds. DSTO-GD-0771 / Cyber Electronic Warfare Division, Defense Science and Technology Organization DSTO. – Edinburgh, Australia, 2013.

12. *Brilingaite A., Bukauskas L., Kutka E.* Development of an educational platform for cyber defence training // Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS'17). – Dublin, Ireland, 2017. – P. 73–81.

Архипова Анастасия Борисовна, доцент кафедры защиты информации Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование в информационной безопасности, оценка качества социально значимой деятельности. E-mail: arhipova@corp.nstu.ru

Бережной Антон Сергеевич, инженер кафедры защиты информации Новосибирского государственного технического университета. Область научных интересов – информационная безопасность. E-mail: kaf_zi@corp.nstu.ru

DOI: 10.17212/2782-2230-2023-3-40-53

Selection and evaluation of functionality of closed program execution environments (sandboxes) for testing and detection of potentially dangerous files and programs*

A.B. Arkhipova[1], A.S. Bereznoy[2]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, Associate Professor of the Department of Information Security. E-mail: arhipova@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, engineer of the Department of Information Security. E-mail: kaf_zi@corp.nstu.ru*

Sandbox technologies provide the most effective mechanisms to protect against targeted and zero-day attacks. The principle of the sandbox is that suspicious software runs in a specially prepared environment for it, isolated from the rest of the infrastructure. The work analyzed the methods for implementing sandboxes to assess and select the functionality of closed environments. We considered local sandboxes, which are part of many antiviruses. They implement isolation based on partial file system virtualization and registry. Analyzed network sandboxes, which have fewer restrictions than local ones, since they do not reduce the performance of the user's computer and allow you to check potential threats on various operating systems. To select and evaluate closed environments, two companies were selected in the work that provide sandboxes both in software and hardware form and using ready-made images for virtualization environments: Fortinet's FortiSandBox and Positive Technologies' PT Sandbox. Product testing took place in demo mode, in a VMware workstation virtual environment.

Keywords: information security, confined environment, sandbox, product testing, virtualization, containerization, functionality, hypervisor

REFERENCES

1. GOST R ISO/MEK 56938–2016. *Zashchita informatsii pri ispol'zovanii tekhnologii virtualizatsii* [State standard R ISO/IEC 56938–2016. Protect information with virtualization technologies]. Moscow, Standards Publ., 2017. 30 p.

2. *Pesochnitsa* [Sandbox]. Kaspersky Lab. (In Russian). Available at: https://www.kaspersky.ru/enterprise-security/wiki-section/products/sandbox (accessed 01.09.2023).

* *Received 10 June 2023.*

3. Kazykhanov A.A., Popov K.G. Analiz ispol'zovaniya pesochnits dlya raboty s zlovredami [Analysis of the use of sandboxes to work with malware]. *Simvol nauki = Symbol of science*, 2016, no. 7-2, pp. 63–64.

4. *Chto takoe pesochnitsa? Kak rabotaet oblachnaya pesochnitsa?* [What is a sandbox? How does the cloud sandbox work?]. Available at: https://www.avast.ru/business/resources/what-is-sandboxing#pc (accessed 04.09.2023).

5. Solopov M.I., Chirkin E.S. Analiz stepeni izolirovannosti zashchishchennykh sred sredstv obespecheniya informatsionnoi bezopasnosti [Analysis of the degree of isolation of protected environments of information security tools]. *Gaudeamus*, 2012, no. 20, pp. 157–159. (In Russian).

6. Byreau Solomatina. *Red Hat Enterprise Virtualization. Obzor produkta* [Red Hat Enterprise Virtualization. Product overview]. Moscow, 2010. Available at: http://www.pcweek.ru/upload/iblock/eba/bureausolomatina-4.pdf (accessed 04.09.2023).

7. Baranov A.V., Nikolaev D.S. Ispol'zovanie konteinernoi virtualizatsii v organizatsii vysokoproizvoditel'nykh vychislenii [The use of container virtualization in the organization of high-performance computing]. *Programmnye sistemy: teoriya i prilozheniya = Software and Systems*, 2016, no. 1 (28), pp. 117–134.

8. Metelkov A.N. Modelirovanie stsenariev kiberatak v kiberpoligonakh [Modeling cyberattack scenarios in cyberpolygons]. *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii = Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia*, 2023, no. 2, pp. 161–176.

9. Metel'kov A.N. Kiberucheniya: zarubezhnyi opyt zashchity kriticheskoi infrastruktury [Cyber exercises: foreign experience in protecting critical infrastructure]. *Pravovaya informatika = Legal Informatics*, 2022, no. 1, pp. 51–60.

10. Virág C., Cegan J., Lieskovan T., Merialdo M. The current state of the art and future of European cyber range ecosystem. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 2021, pp. 390–395.

11. Davies J., Margat S. *A survey of cyber ranges and testbeds*. DSTO-GD-0771. Cyber Electronic Warfare Division, Defense Science and Technology Organization DSTO, Edinburgh, Australia, 2013.

12. Brilingaite A., Bukauskas L., Kutka E. Development of an educational platform for cyber defence training. *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS'17)*, Dublin, Ireland, 2017, pp. 73–81.

Для цитирования:

Архипова А.Б., *Бережной А.С.* Выбор и оценка функциональности замкнутых сред выполнения программ («песочниц») для тестирования и детектирования потенциально опасных файлов и программ // Безопасность цифровых технологий. – 2023. – № 3 (110). – С. 40–53. – DOI: 10.17212/2782-2230-2023-3-40-53.

For citation:

Arkhipova A.B., Bereznoy A.S. Vybor i otsenka funktsional'nosti zamknutykh sred vypolneniya programm («pesochnits») dlya testirovaniya i detektirovaniya potentsial'no opasnykh failov i programm [Selection and evaluation of functionality of closed program execution environments (sandboxes) for testing and detection of potentially dangerous files and programs]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 3 (110), pp. 40–53. DOI: 10.17212/2782-2230-2023-3-40-53.