

УДК 004.056.5

М. А. БУХОВЕЦ, Н. В. ГРИГОРЬЕВ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН,*
С. С. ТАТУР

ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ИЗОЛИРОВАННОЙ СРЕДЕ

Рассмотрены методики выявления скрытых угроз в исполняемых файлах, распространяемых через неофициальные ресурсы. Проведён сравнительный анализ поведения троянского компонента, замаскированного под игровой модификатор, и профессионального образца вредоносного кода из открытой базы MalwareBazaar [3]. Для изучения применялись автоматизированная песочница Cuckoo Sandbox [1] и специализированный дистрибутив REMnux [2]. Экспериментальная часть включала запуск образцов в изолированной виртуальной машине с фиксацией сетевых запросов, изменений реестра и файловой системы. Установлены характерные признаки закрепления угроз в операционной системе и техники обхода средств защиты. Результаты подтверждают необходимость строгой изоляции при исследовании подозрительных файлов и демонстрируют эффективность динамического анализа для своевременного выявления индикаторов компрометации.

В научной литературе и практике информационной безопасности акцент традиционно смещён в сторону статического анализа исполняемых файлов. Однако современные угрозы активно применяют полиморфное шифрование, упаковку и техники антиотладки, что существенно снижает результативность сигнатурных методов. В условиях расширения цифровых сервисов пользователи регулярно сталкиваются с файлами, распространяемыми вне официальных источников, и добровольно отключают средства защиты перед их запуском, что создаёт благоприятную среду для компрометации рабочих станций. Динамический анализ в контролируемой среде позволяет зарегистрировать фактическую активность кода без риска заражения основной инфраструктуры, однако на практике недостаточно систематизированы поведенческие различия между любительскими угрозами массового распространения и профессиональными загрузчиками. Цель работы заключается в сравнительном исследовании поведения двух классов угроз, выявлении характерных индикаторов компрометации, верификации автоматизированных отчётов ручным тестированием и формировании практических рекомендаций по безопасному изучению подозрительных программ.

Методология исследования и организация лабораторной среды.

Для проведения экспериментов создана изолированная лабораторная среда на базе гипервизора. Виртуальная машина с операционной системой

Windows 10 настроена с отключённым сетевым адаптером или переведена в режим внутренней сети, что исключает утечку данных на внешние узлы и предотвращает нецелевое распространение индикаторов компрометации. Перед каждым запуском формируется контрольный снимок состояния системы, позволяющий мгновенно восстановить исходную конфигурацию после завершения теста.

Анализ проводился в дистрибутиве REMnux [2], содержащем набор утилит для предварительной обработки файлов: ClamAV, sara, strings, PEScanner. Данные инструменты обеспечивают быстрое извлечение строковых литералов, определение упаковщиков и выявление подозрительных импортируемых функций без выполнения кода. Поведенческое исследование реализовано через платформу Cuckoo Sandbox [1], которая автоматически разворачивает целевой процесс в изолированном окружении, мониторит системные вызовы, фиксирует обращения к реестру, создание файлов, модификацию служб и сетевые соединения. Результаты генерируются в виде структурированных отчётов с временными метками и хэшами индикаторов.

Результаты анализа образца из публичного источника.

Первый тестовый файл распространялся на игровом форуме под наименованием AstroUnlocker.rar и позиционировался как инструмент разблокировки дополнительного контента. Пользовательские комментарии содержали прямые указания на срабатывание средств защиты, что служит первичным индикатором потенциальной угрозы. Предварительная проверка через ClamAV и агрегатор VirusTotal [4] подтвердила наличие детектирования множеством вендоров по сигнатуре Trojan.Agent.

После загрузки архива в песочницу зафиксирована следующая активность: создание копии исполняемого файла в директории %AppData%\Local\Temp с последующим скрытием атрибутов; модификация раздела HKCU\Software\Microsoft\Windows\CurrentVersion\Run для обеспечения автозапуска после перезагрузки системы; установка исходящих соединений на порты 443 и 8080 к внешним IP-адресам, не связанным с официальными серверами игровых платформ; попытка обращения к планировщику заданий для периодической проверки наличия обновлений на управляющем сервере. Отчёт Cuckoo Sandbox [1] продемонстрировал отсутствие взаимодействия с игровыми процессами. Функционал, заявленный разработчиком, не реализован. Зафиксированная активность соответствует поведению трояна удалённого доступа, предназначенного для сбора системной информации и получения команд от внешнего оператора.

3 Сравнительное исследование с профессиональным загрузчиком.

Второй этап исследования посвящён анализу файла, загруженного через официальный интерфейс MalwareBazaar [3] (хэш SHA-256: 3ca9b4e8...) (рисунк 1). Данный образец относится к категории загрузчиков и демонстрирует усложнённую архитектуру взаимодействия с операционной системой.

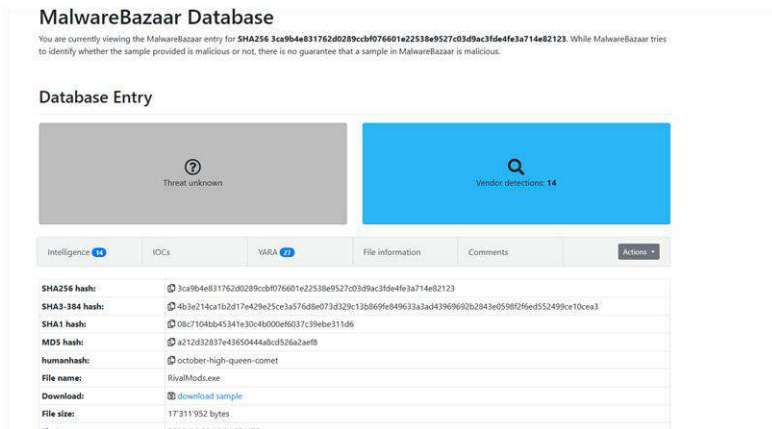


Рисунок 1 – Страница образца RivalMods.exe в базе MalwareBazaar с детектированием 14 антивирусными движками

Сравнительные характеристики деятельности игрового модификатора и загрузчика из MalwareBazaar обоих образцов представлены в таблице 1. Образец из профессиональной базы демонстрирует многоэтапную стратегию обхода контроля.

Таблица 1 – Сравнительный анализ поведения исследуемых образцов

Параметр мониторинга	Образец 1 (игровой модификатор)	Образец 2 (загрузчик из MalwareBazaar)
Сетевая активность	Единичное подключение к одному неизвестному IP/домену (C2-сервер)	Использование нескольких резервных каналов связи с управляющими серверами
Действия файловой системой	Создание скрытой копии исполняемого файла в директории %AppData%	Акцент смещён на манипуляции с процессами; файловые операции не являются приоритетными
Механизмы закрепления	Прописывание записи в реестре или планировщике задач для обеспечения автозапуска	Реализуются стандартные методы, но в отчёте акцент сделан на процессном взаимодействии
Техники сокрытия и обхода защиты	Отсутствуют; программа работает в фоновом режиме без противодействия средствам безопасности	Инъекция кода в легитимные системные процессы; принудительное завершение процессов антивирусов; попытки отключения Windows Defender
Итоговая классификация по результатам анализа	Троян удалённого доступа или базовый загрузчик, предназначенный для массового распространения	Продвинутый загрузчик с многоэтапной логикой противодействия статическому и динамическому анализу

Зафиксировано применение техник инъекции кода в системные процессы, что усложняет визуальное обнаружение через диспетчер задач. Сетевой трафик структурирован с применением чередующихся доменов, что повышает устойчивость канала управления при блокировке отдельных узлов. Отключение средств защиты выполняется через модификацию групповых политик и служб безопасности, тогда как первый образец взаимодействует с системой без применения агрессивных методов противодействия.

Верификация автоматизированных отчётов в изолированной среде.

Для подтверждения автоматизированных отчётов проведён ручной запуск первого образца в чистой виртуальной машине. До запуска сделан снимок состояния системы. После выполнения исполняемого файла зафиксированы изменения в оснастке regedit (созданный ключ автозапуска), появление скрытого каталога в %AppData%, а также наличие подозрительного процесса в диспетчере задач, потребляющего ресурсы в фоновом режиме.

Попытка установки исходящего соединения заблокирована брандмауэром Windows, что подтверждает наличие внешнего канала связи. Восстановление системы из сохранённого снимка заняло менее 15 секунд и полностью устранило внесённые изменения. Процедура подтвердила корректность данных, полученных песочницей, и продемонстрировала эффективность изолированного тестирования для предотвращения необратимого заражения.

Проведённое исследование выявило характерные признаки маскировки вредоносного кода под игровые утилиты и установило различия в технике взаимодействия с операционной системой у образцов разной сложности. Первый файл реализует базовый сценарий закрепления и связи с управляющим сервером, тогда как профессиональный загрузчик применяет многоуровневую защиту, инъекцию в системные процессы и методы обхода средств безопасности.

Научная новизна работы заключается в систематизации индикаторов компрометации для конкретных классов угроз и демонстрации последовательности верификации автоматизированных данных ручным тестированием в виртуальной среде. Преимущество предложенной методики состоит в сочетании статической предварительной проверки, динамического анализа в песочнице и изолированного запуска, что исключает ложные срабатывания и снижает риск компрометации исследовательской инфраструктуры.

Практическая ценность результатов определяется возможностью использования выявленных шаблонов поведения для настройки правил корреляции в системах мониторинга безопасности, формирования учебных сценариев по анализу вредоносных программ и разработки рекомендаций по минимизации угроз при работе с непроверенным ПО.

СПИСОК ЛИТЕРАТУРЫ

- 1 Cuckoo Sandbox Documentation. – URL: <https://cuckoosandbox.org/> (date of access: 28.04.2026).
- 2 REMnux: A Linux Toolkit for Malware Analysts. – URL: <https://remnux.org/> (date of access: 28.04.2026).
- 3 Abuse.ch // MalwareBazaar. – URL: <https://bazaar.abuse.ch/> (дата обращения: 28.04.2026).
- 4 Chronicle Security // VirusTotal. – URL: <https://www.virustotal.com/> (date of access: 28.04.2026).
- 5 Playground.ru: Форум пользователей. – URL: <https://forum.playground.ru/> (date of access: 28.04.2026).

Получено 25.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 656.21:623.746.4-519

Е. В. БЫВШЕВ (УД-21)

Научный руководитель – канд. техн. наук *В. Г. КУЗНЕЦОВ*

ДРОНИФИКАЦИЯ НА ЖЕЛЕЗНОДОРОЖНОЙ СТАНЦИИ

Проведен анализ процессов эксплуатационной работы на железнодорожной станции, а также возможности применения специальных дронов для выполнения отдельных операций. Даны примеры практического применения дронов на железнодорожной станции.

На железнодорожном транспорте активно реализуются технические и технологические мероприятия, направленные на автоматизацию и механизацию станционных процессов. Одним из инновационных способов, который позволяет ускорить выполнение операций на станциях, а также повысить безопасность труда, является «дронификация». Под этим термином понимают процесс использования специализированных устройств (дронов) для выполнения различных операций на объектах. Такая технология использования дронов активно применяется во многих отраслях экономики страны.

Дроны оснащаются устройствами, которые позволяют реализовать следующий функционал: автоматическое считывание данных, мониторинг местности, транспортировка предметов и др. Дроны, оборудованные устройствами LIDAR и RTK-навигацией, способствуют созданию точных цифровых моделей местности и дают возможность создать достоверные