

УДК 004.056.5

Д. А. ЧЕПКО, А. С. ИВОЛГА (ЭМ-21)

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

АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ МУЛЬТИСКАНЕРНОГО ОНЛАЙН-СЕРВИСА VIRUSTOTAL ДЛЯ ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Произведен комплексный анализ функциональных возможностей и архитектурных ограничений онлайн-сервиса VirusTotal как инструмента для вторичной диагностики файлов, URL-адресов и хеш-сумм. Исследована методология формирования отчетов на основе агрегации данных более 70 антивирусных движков и систем песочниц. Определены критерии оценки релевантности результатов сканирования с учетом весовых коэффициентов и репутации антивирусных лабораторий. Рассмотрены сценарии использования сервиса для различных категорий пользователей, включая ИТ-специалистов и исследователей кибербезопасности, а также выявлены ключевые риски, связанные с обработкой конфиденциальных данных в публичной среде.

В условиях экспоненциального роста числа сложных целенаправленных атак (APT) и увеличения объема полиморфного вредоносного программного обеспечения, традиционные методы защиты, основанные на использовании изолированных антивирусных решений, часто демонстрируют недостаточную эффективность. Это особенно характерно для угроз нулевого дня (zero-day) или модифицированных образцов, не имеющих сигнатур в локальных базах данных. Возникает проблема «ложного чувства безопасности», когда штатное антивирусное ПО не детектирует угрозу, что обуславливает необходимость применения инструментов для получения независимого «второго мнения» на основе коллективного интеллекта.

Актуальность исследования заключается в необходимости систематизации знаний о возможностях публичных агрегаторов угроз и выработки четких методических рекомендаций по интерпретации их результатов для минимизации рисков компрометации корпоративных информационных систем.

Цель работы – провести глубокий анализ архитектуры и методологии работы сервиса VirusTotal, определить его место в системе обеспечения информационной безопасности и разработать критерии для качественной оценки достоверности результатов сканирования.

В рамках исследования VirusTotal рассматривается не как классическая система защиты конечных точек (endpoint protection), работающая в режиме реального времени (on-access scanning), а как веб-платформа, выполняющая

функции агрегатора телематических данных и многовекторной проверки. Архитектура сервиса предполагает распределение загруженного пользователем объекта (исполняемый файл, документ, архив, URL-адрес или хеш-сумма MD5/SHA-1/SHA-256) между 60–70 интегрированными сканерами. Партнерская сеть включает ведущих разработчиков средств защиты информации, таких как «Лаборатория Касперского», Bitdefender, Microsoft, ESET и др.

Выделяют три основных сценария взаимодействия с платформой:

1 Проверка файла – загрузка подозрительного объекта для статического анализа и динамического выполнения в изолированной среде (песочнице).

2 Проверка URL – анализ веб-адреса через безопасную эмуляцию перехода (headless browser), проверку репутации домена и анализ DOM-дерева страницы.

3 Поиск по хешу – идентификация ранее проанализированных объектов без повторной загрузки, что позволяет экономить сетевой трафик и время при работе с большими массивами данных, а также интегрировать сервис в SIEM-системы через API.

Ключевым этапом работы с сервисом является интерпретация сформированного отчета. Основным визуальным индикатором выступает соотношение количества детектов к общему числу задействованных сканеров (например, «15 из 70»). Однако проведенный анализ показывает, что количественный показатель не является абсолютным критерием истины. Решающим фактором выступает качественный состав детектов и репутация вендоров.

Если сигнатуры сработали исключительно у малоизвестных или нишевых антивирусных продуктов, в то время как лидеры рынка классифицируют файл как безопасный, с высокой долей вероятности имеет место ложноположительное срабатывание (false positive), что характерно для новых легитимных утилит или самописного ПО. Обратная ситуация, когда файл блокируется ведущими вендорами (Kaspersky, Bitdefender, Symantec), является критическим маркером угрозы, даже если общее число детектов не превышает 20–30 % от общего количества сканеров.

Дополнительными факторами верификации, повышающими достоверность оценки, являются метаданные объекта: история загрузок, поведенческий анализ в песочнице (фиксирующий попытки модификации реестра, создания процессов автозагрузки, инъекций в легитимные процессы или установления сетевых соединений с командными центрами C2), а также комментарии сообщества исследователей и привязка к правилам YARA.

Для иллюстрации методологии рассмотрим типичный сценарий целевой атаки. Пользователь получает электронное письмо от имени службы безопасности с вложенным исполняемым файлом. Локальное антивирусное ПО не выявляет угроз. При загрузке файла в VirusTotal фиксируется результат: 15 детектов из 70. Количественно это не выглядит как критическая угроза. Однако качественный анализ показывает, что среди сработавших движков присутствуют Kaspersky, Bitdefender и Microsoft Defender. Дополнительно раздел «Поведение в песочнице» демонстрирует попытки файла прописать

себя в автозагрузку Windows (Registry Run Keys) и инициировать исходящие соединения с неизвестным IP-кодом по порту 443. Совокупность этих факторов однозначно классифицирует объект как вредоносный, предотвращая заражение рабочей станции.

Несмотря на высокую эффективность, использование сервиса сопряжено с рядом существенных ограничений и рисков. Во-первых, платформа имеет двойное назначение: наряду с защитными целями, она активно используется злоумышленниками для тестирования собственных образцов вредоносного ПО на предмет обнаружения антивирусами перед запуском целевых кампаний (AV evasion testing). Во-вторых, и это является наиболее критичным ограничением, загружаемые данные становятся публичными. Компания VirusTotal делится образцами файлов и метаданными со своими партнерами по кибербезопасности. Следовательно, категорически недопустимо использование сервиса для проверки файлов, содержащих конфиденциальную информацию, персональные данные (в разрезе требований законодательства о защите персональных данных), коммерческую тайну или служебную документацию. В-третьих, сервис выполняет исключительно диагностическую функцию и не способен нейтрализовать угрозу в системе пользователя, требуя наличия активных средств защиты.

По результатам проведенного исследования сформулированы следующие выводы: VirusTotal является высокоэффективным дополнением к стационарным антивирусным системам, позволяющим валидировать подозрительные объекты, но не может служить их полной заменой из-за отсутствия защиты в реальном времени. Эффективность использования сервиса напрямую зависит от квалификации пользователя: критически важна не доля «красных» отметок, а репутация и вес сработавших антивирусных движков, подкрепленные данными поведенческого анализа в песочнице. Применение сервиса в корпоративной среде требует строгого соблюдения политик информационной безопасности, исключающих загрузку конфиденциальных данных в публичные облачные среды, и должно быть регламентировано внутренними инструкциями. Интеграция VirusTotal API в корпоративные SOC-центры позволяет автоматизировать процесс первичного триажа инцидентов, значительно сокращая время реакции на потенциальные угрозы.

СПИСОК ЛИТЕРАТУРЫ

1 VirusTotal. Documentation and API Reference. – URL: [https:// developers. virustotal.com](https://developers.virustotal.com). (date of access: 20.05.2025).

2 **Ховард, Р.** Кибербезопасность: главные принципы / Р. Ховард. – СПб. : Питер, 2024. – 320 с.

3 **Кузнецов, А. В.** Информационная безопасность: анализ и оценка угроз, кибер/криптозащита организаций, разработка безопасного ПО / А. В. Кузнецов. – М. : Наука и техника, 2025. – 432 с.

Получено 28.05.2026