УДК 004.056

МНОГОЭТАПНАЯ КОМПРОМЕТАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ: ВЗЛОМ ВЕБ-API И ГЕНЕРАТИВНАЯ ОБФУСКАЦИЯ ПОЛЕЗНОЙ НАГРУЗКИ

М.А. Винокуров, Д.А. Шумило
Учреждение образования «Гомельский Государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В статье исследуется комплексный сценарий современных кибератак, включающий этапы сетевого проникновения и исполнения вредоносного кода. Проанализированы недостатки стандартных модулей Metasploit Framework при обходе WAF и обосновано применение Python-скриптов для тестирования веб-API. Рассмотрен концептуально новый метод доставки полезной нагрузки после проникновения, основанный на генеративной обфускации с использованием локальных языковых моделей (LLM). Обоснована необходимость перехода от сигнатурного к поведенческому мониторингу на всех уровнях инфраструктуры.
Ключевые слова: веб-приложение; API; WAF; тестирование на проникновение; Metasploit Framework; обход защиты; генеративная обфускация; большая языковая модель; поведенческий анализ; информационная безопасность.

MULTISTAGE COMPROMISE OF INFORMATION SYSTEMS: WEB API HACKING AND GENERATIVE PAYLOAD OBFUSCATION

Vinokurov M., Shumilo D.
Educational Institution "Francysk Skaryna Gomel State University", Gomel, Republic of Belarus

Abstract. The article explores a complex scenario of modern cyberattacks, including the stages of network penetration and malicious code execution. The shortcomings of standard Metasploit Framework modules in bypassing WAF are analyzed, and the use of Python scripts for testing web APIs is justified. A conceptually new method of payload delivery after penetration, based on generative obfuscation using local large language models (LLMs), is considered. The necessity of transitioning from signature-based to behavioral monitoring at all infrastructure levels is substantiated.
Keywords: web application; API; WAF; penetration testing; Metasploit Framework; defense bypass; generative obfuscation; large language model; behavioral analysis; information security.

Введение

Современные информационные системы сталкиваются с угрозами, реализующими многовекторный подход к обходу защиты. Эффективная кибератака сегодня – это не единичное действие, а строго выверенная цепочка, где злоумышленникам необходимо преодолеть как минимум два рубежа: сетевой периметр и средства защиты конечных точек. В условиях стремительного развития защитных механизмов киберпреступники вынуждены непрерывно совершенствовать тактики скрытного

присутствия. Это приводит к формированию комплексных сценариев компрометации, где на каждом шаге применяются специфические, зачастую неочевидные методы уклонения от мониторинга. Наибольшую опасность в таких сценариях представляют комбинированные техники, эксплуатирующие уязвимости программных интерфейсов (API) для первичного сетевого доступа, с последующим применением алгоритмов машинного обучения для маскировки исполнения вредоносного кода непосредственно внутри атакованной инфраструктуры.

Основная часть

В современной микросервисной архитектуре основным вектором начального доступа выступают веб-API. Злоумышленники активно используют методы автоматизированного перебора, однако классический брутфорс оперативно блокируется межсетевыми экранами уровня приложений. Современные системы защиты анализируют не только частоту запросов, но и цифровые отпечатки протокола TLS (JA3/JA3S), а также поведенческие паттерны.

Проведение качественного аудита безопасности в таких условиях требует адекватного инструментария. Практика показывает, что стандартные средства тестирования на проникновение, включая многие базовые модули платформы Metasploit Framework, демонстрируют недостаточную гибкость. Они обладают жесткой архитектурой отправки запросов и легко детектируются по характерным сетевым сигнатурам. Для успешной эмуляции современных атак требуется разработка кастомного инструментария. В частности, встроенные сканеры испытывают критические сложности с фаззингом многоуровневых JSON-объектов и запросов GraphQL, что делает практически невозможным поиск уязвимостей нарушения авторизации на уровне свойств объектов.

Разработка специализированных модулей на языке Python для среды Metasploit позволяет решить эту проблему за счет реализации интеллектуального парсинга ответов API и автоматического извлечения, и обновления JWT-токенов «на лету». Кроме того, применение асинхронных Python-библиотек дает возможность генерировать распределенный сетевой трафик через пулы резидентных прокси. Это обеспечивает надежный обход алгоритмов, используемых современными API-шлюзами для динамического ограничения запросов, не вызывая подозрений у аналитических систем WAF.

После успешного проникновения через API (например, получения RCE-уязвимости или доступа с правами администратора) перед атакующим встает задача скрытной доставки полезной нагрузки. На этом этапе классические методы обфускации (упаковщики, шифровальщики) теряют эффективность: зашифрованный файл обладает аномально высокой

энтропией, что моментально выявляется современными ML-детекторами антивирусных систем.

Решением для злоумышленников стало использование больших языковых моделей. Новый подход отказывается от сокрытия уже написанного вредоносного кода – вместо этого ИИ синтезирует его непосредственно на атакованном узле. Схема атаки выглядит следующим образом: через уязвимый API на сервер загружается легитимная, на первый взгляд, программа-загрузчик, содержащая штатные библиотеки для работы с машинным обучением (например, onnxruntime.dll) и файл с весами локальной нейросети. Статические сканеры не видят в этом наборе угрозы. В момент запуска загрузчик собирает телеметрию системы (версию ОС, открытые порты, установленные утилиты) и передает их в качестве инструкции нейросети. В свою очередь, языковая модель, предварительно дообученная злоумышленниками на генерацию эксплойтов, синтезирует уникальный вредоносный код прямо в оперативной памяти.

В результате вредоносная логика скрывается не в шифрованном архиве, а в миллиардах числовых параметров (весах) матриц модели ИИ. Процесс дообучения становится высшей формой обфускации. Извлечь вредоносную сигнатуру из матриц весов статическим анализом технически невозможно – это абсолютный черный ящик.

Заключение

Таким образом, современные атаки на веб-приложения характеризуются глубокой маскировкой на каждом этапе своего жизненного цикла. На уровне сети (при атаке на API) применение гибких скриптов на Python позволяет злоумышленникам обходить WAF, полностью имитируя поведение легитимных клиентов. На уровне хоста (при исполнении полезной нагрузки) использование дообученных языковых моделей сводит на нет эффективность антивирусных сканеров, маскируя вирус под легитимные процессы машинного обучения.

Анализ этих векторов доказывает, что парадигма статической защиты окончательно устарела. Обеспечение безопасности требует концептуального перехода к динамическому контролю инфраструктуры. Эффективная защита возможна только путем непрерывного поведенческого мониторинга: выявления нетипичной последовательности вызовов API на сетевом шлюзе, а также блокировки бесфайлового исполнения кода и аномальных пиков потребления вычислительных ресурсов (CPU/GPU) на конечных узлах.

Сведения об авторах

Винокуров М.А., студент 4-го курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования

«Гомельский государственный университет имени Франциска Скорины», maks_vinokurov_2005@mail.ru.

Шумило Д.А., студент 4-го курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», shmain125@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Vinokurov M., 4th year student of the Faculty of Physics and Information Technology specialty "Computer security", Educational Institution "Francysk Skaryna Gomel State University", maks_vinokurov_2005@mail.ru.

Shumilo D., 4th year student of the Faculty of Physics and Information Technology specialty "Computer security", Educational Institution "Francysk Skaryna Gomel State University", shmain125@gmail.com.

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Educational Institution "Francysk Skaryna Gomel State University", vaskevich@gsu.by.