DOI: 10.37791/2687-0649-2021-16-2-103-122

Анализ и совершенствование методов обнаружения шелл-кодов (shellcode) в компьютерных системах

В. В. Ерохин[1*], ***Л. С. Притчина***[1]
[1] *Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, Москва, Россия*
** erohinvv@mail.ru*

Аннотация. В статье рассматривается проблема обнаружения и фильтрации шелл-кодов (shellcode) – вредоносного исполняемого кода, способствующего появлению уязвимостей при работе программных приложений с памятью. Основными такими уязвимостями являются переполнение стека, переполнение баз данных, а также некоторых других служебных процедур операционной системы. В настоящее время существует несколько десятков систем обнаружения шелл-кодов, использующих как статический, так и динамический анализ программ. Мониторинг существующих систем показал, что методы, обладающие невысокой вычислительной сложностью, характеризуются большим процентом ложных срабатываний. При этом методы с невысоким процентом ложных срабатываний характеризуются повышенной вычислительной сложностью. Однако ни одно из существующих на настоящий момент решений не в состоянии обнаруживать все существующие классы шелл-кодов. Это делает существующие системы обнаружения шелл-кодов слабо применимыми к реальным сетевым каналам. Таким образом, в статье рассмотрена задача анализа систем обнаружения шелл-кодов, обеспечивающих полное обнаружение существующих классов шелл-кодов и характеризующихся приемлемой вычислительной сложностью и малым количеством ложных срабатываний. Представлены классификации шелл-кодов и комплексный метод их обнаружения, основанный на эмуляции кода. Этот подход расширяет диапазон детектирования классов шелл-кодов, которые могут быть обнаружены, за счет параллельной оценки нескольких эвристик, которые соответствуют низкоуровневым операциям на CPU во время выполнения различных классов шелл-кода. Представленный метод позволяет эффективно обнаруживать простой и метаморфический шелл-код. Это достигается независимо от использования самомодифицируемого кода или генерации динамического кода, на которых основаны существующие детекторы полиморфного шелл-кода на основе эмуляции.

Ключевые слова: информационная безопасность, шелл-код, классификация вредоносных программ, обнаружение шелл-кода, компьютерная система, эмуляция кода

Для цитирования: *Ерохин В. В., Притчина Л. С.* Анализ и совершенствование методов обнаружения шелл-кодов (shellcode) в компьютерных системах // Прикладная информатика. 2021. Т. 16. № 2. С. 103–122. DOI: 10.37791/2687-0649-2021-16-2-103-122

Analysis and improvement of methods for detecting shellcodes in computer systems

V. Erokhin[1*], ***L. Pritchina***[1]
[1] *Moscow State Institute of International Relations (MGIMO), Moscow, Russia*
** erohinvv@mail.ru*

Abstract. The article discusses the problem of detecting and filtering shellcode – malicious executable code that contributes to the emergence of vulnerabilities in the operation of software applications with memory. The main such vulnerabilities are stack overflow, database overflow, and some other operating system service procedures. Currently, there are several dozen shellcode detection systems using both static and dynamic program analysis. Monitoring of existing systems has shown that methods with low computational complexity are characterized by a large percentage of false positives. Moreover, methods with a low percentage of false alarms are characterized by increased computational complexity. However, none of the currently existing solutions is able to detect all existing classes of shellcodes. This makes existing shellcode detection systems weakly applicable to real network links. Thus, the article discusses the problem of analyzing shellcode detection systems that provide complete detection of existing classes of shellcodes and are characterized by acceptable computational complexity and a small number of false alarms. This article introduces shellcode classifications and a comprehensive method of detecting them based on code emulation. This approach expands the detection range of shellcode classes that can be detected by concurrently evaluating several heuristics that correspond to low-level CPU operations during execution of various shellcode classes. The presented method allows efficient detection of simple and metamorphic shellcode. This is achieved regardless of the use of self-modifying code or dynamic code generation on which existing emulation-based polymorphic shellcode detectors are based.

Keywords: information security, shellcode, malware classification, shellcode detection, computer system, code emulation

For citation: Erokhin V., Pritchina L. Analysis and improvement of methods for detecting shellcodes in computer systems. *Prikladnaya informatika*=Journal of Applied Informatics, 2021, vol.16, no.2, pp.103-122 (in Russian). DOI: 10.37791/2687-0649-2021-16-2-103-122

Введение

Дистанционно запускаемые программные шелл-коды – это распространенный способ проникновения злоумышленников в уязвимые компьютерные системы. По мере совершенствования методов обнаружения развиваются и методы удаленной эксплуатации [2]. Недавние методы уклонения от обнаружения шелл-кодов включают полиморфизм (шифрование кода) и метаморфизм (обфускация кода).

Полиморфные черви нулевого уровня представляют серьезную угрозу безопасности интернет-инфраструктур. Учитывая их быстрое распространение, очень важно обнаруживать их в пограничных сетях и автоматически генерировать оповещения на ранних стадиях заражения. Большинство существующих подходов для автоматической генерации оповещений о заражении программного кода или сетевого трафика требуют информации о хосте и, следовательно, не применимы для развертывания в высокоскоростных сетевых соединениях.