УДК 004.432.2

АНАЛИЗ МЕТОДОВ СОКРЫТИЯ ПОЛЕЗНОЙ НАГРУЗКИ В POWERSHELL-СКРИПТАХ

А.В. Павлов

(Университет ИТМО, г. Санкт-Петербург)

Научный руководитель – к.т.н., доцент Волошина Н.В.

(Университет ИТМО, г. Санкт-Петербург)

На сегодняшний день система каталогов Active Directory от Microsoft занимает доминантное положение на рынке. Её доля составляет, по разным оценкам, от 90 до 95 процентов. Основной язык автоматизации процессов в Active Directory – PowerShell. Именно его зачастую используют злоумышленники при пост-эксплуатации системы. При анализе защищенности контура Active Directory важно понимать, какими методами атакующие могут пользоваться с целью сокрытия полезной нагрузки в PowerShell-скриптах.

Целью работы стал анализ существующих методов сокрытия полезной нагрузки в PowerShell-скриптах и возможности их обнаружения в ходе машинного и ручного анализа.

В работе рассматриваются существующие методы встраивания для PowerShell-скриптов:

- обфускация на основании смешивания регистров;
- обфускация на методе переопределения порядка и вызовов;
- методы, основанные на кодировании;
- стеганографические (мимикрические) методы встраивания;
- комбинированный подход.

Рассмотрены подходы к машинному анализу скриптов, ситуации и паттерны ручного анализа. Исследована возможность обнаружения полезной нагрузки.

В результате работы описаны различные подходы к сокрытию полезной нагрузки, методы выявления встраивания и рекомендации по настройке систем защиты Active Directory-контура.