Лукин Евгений Игоревич

Факультет информатики
и прикладной математики

II курс
ИБ-1601 группа

Научный руководитель – доцент кафедры
вычислительных систем и программирования
Чернокнижный Геннадий Михайлович

АНАЛИЗ УГРОЗ БОТНЕТ И РАЗРАБОТКА ПРИКЛАДНЫХ СРЕДСТВ ОБНАРУЖЕНИЯ БОТНЕТ-АГЕНТА

Аннотация. В работе была поставлена и решена задача разработки комплекса средств обнаружения ботнет-агента с использованием существующих и оригинальных (разработанных автором) программных продуктов. Для решения задачи была создана ботнет-сеть и смоделирована ботнет-атака на рабочую станцию с удаленного физического сервера, в которой документировалось нажатие клавиш на клавиатуре атакуемой станции и делались снимки экрана. Информация передавалась на сторонний сервер. Ботнет-агент, сервер управления и контроля, а также ряд программ обнаружения ботнет-агента программно созданы автором на различных языках программирования. Для анализа и поиска зловредного агента в системе использованы известные анализаторы и программы-мониторы.

Ключевые слова: ботнет-сеть, ботнет-атака, удаленный сервер, программа обнаружения.

Abstract. The task of developing a complex of tools for detecting botnet agent using existing and original (developed by the author) software products was set and solved in the work. To solve the problem, a botnet network was created and a botnet attack on a workstation from a remote physical server was simulated, in which keystrokes on the keyboard of the attacked station were documented and screen shots were taken. The information was transmitted to a third-party server. Botnet agent, management and control server, as well as a number of botnet agent detection programs are created by the author in various programming languages. To analyze and find a malicious agent in the system, known analyzers and monitor programs were used.

Keywords: Botnet-a network, a botnet attack, a remote server, the program detection.

Контактная информация автора работы: genya.lukin@yandex.ru