J Inf Process Syst
http://dx.doi.org/10.3745/JIPS.03.0026

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

WebSHArk 1.0: A Benchmark Collection for Malicious Web Shell Detection

Jinsuk Kim*, Dong-Hoon Yoo*,**, Heejin Jang*, and Kimoon Jeong*

Abstract

Web shells are programs that are written for a specific purpose in Web scripting languages, such as PHP, ASP, ASP.NET, JSP, PERL-CGI, etc. Web shells provide a means to communicate with the server's operating system via the interpreter of the web scripting languages. Hence, web shells can execute OS specific commands over HTTP. Usually, web attacks by malicious users are made by uploading one of these web shells to compromise the target web servers. Though there have been several approaches to detect such malicious web shells, no standard dataset has been built to compare various web shell detection techniques. In this paper, we present a collection of web shell files, WebSHArk 1.0, as a standard dataset for current and future studies in malicious web shell detection. To provide baseline results for future studies and for the improvement of current tools, we also present some benchmark results by scanning the WebSHArk dataset directory with three web shell scanning tools that are publicly available on the Internet. The WebSHArk 1.0 dataset is only available upon request via email to one of the authors, due to security and legal issues.

Keywords

Benchmark Test Collection, Malicious Web Application, Webshell, Web Shell Collection, Web Shell Detection

1. Introduction

As of January 2014, there was more than 861 million websites [1] operated every day for both personal and professional use. Being so common, these websites have high chances of becoming targets of web attacks by malicious hackers. Out of web attacks, uploading web shells to the target websites is the most widespread means of compromising and exploiting the victim server. There has been a report that one or more malicious web shells are found in 91% of hacked websites in South Korea [2].

Malicious web shells are small programs or scripts that can be opened from a web browser to provide a web-based interface to run OS specific system commands. These run purely over the WWW via HTTP protocol. Usually, web shells provide a quick GUI interface to do one or more of the following common tasks: 1) executing OS shell commands, 2) traversing across directories, 3) viewing files, 4) editing files, 5) downloading files, 6) deleting files, 7) uploading files, 8) executing DB SQL queries and commands, 9) bypassing mod_security, 10) sending spam mails, 11) running IRC bots, and 12)

Manuscript received February 25, 2014; accepted April 16, 2014.
Corresponding Author: Kimoon Jeong (kmjeong@kisti.re.kr)
* Department of Science &Technology Security, National Institute of Supercomputing & Networking (NISN), Korea Institute of Science &Technology Information (KISTI), Daejeon 305-806, Korea ({jinsuk, jhj, x82, kmjeong}@kisti.re.kr)
** Department of Computer Engineering, Chonnam National University, Gwangju 500-757, Korea (x82@kisti.re.kr)