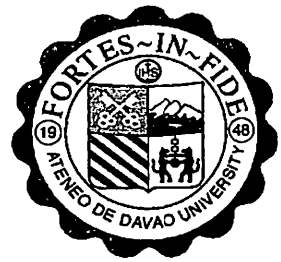

ATENEO DE DAVAO UNIVERSITY
Computer Studies Division

Mini-Thesis

A FRAMEWORK OF DETECTION AND PREVENTION OF mIRC®-TRIGGERED MALICIOUS WEB SCRIPTS

Group Name: SINGING BABA BEAR

Proponents: AMBULO, REYNANN PAUL
SANTILLAN, IANNICAR GRACE
SANTOS, KENNETH CARLO

Course: Bachelor of Science in Computer Science

School Year: SY 2003 -2004

A FRAMEWORK OF DETECTION AND PREVENTION OF mIRC®-TRIGGERED MALICIOUS WEB SCRIPTS

A Mini-Thesis
Presented to
The Faculty of the Computer Science Division
Ateneo de Davao University

In Partial Fulfillment
Of the Requirements for the Degree
Bachelor of Science, Major in Computer Science

By:

Reynann Paul Ambulo
Iannicar Grace Santillan
Kenneth Carlo Santos

March 2004

TABLE OF CONTENTS

Page

ABSTRACT

The growth of the Internet community in the Philippines has opened a door for intruders to come in. There is a new rampant form of attack that is now being used on web browsers that of which effects are rather frustrating and more irritating than the usual virus. It is rather difficult to detect this problem because it can disguise itself as an ordinary script in a computer. The problem mostly arises from the use of mIRC® where the web address is advertised. There are many possible security solutions to this problem but most of them are too broad for its scope. Businesses such as Internet Café's are asked for licenses from the government to prove the legality of their software. Nowadays it is still expensive for them to buy the licenses here in the Philippines.

Keywords: *malicious script, mIRC® script, Trojan, ad-ware, web browsers*

Chapter 1
Introduction

1.1 Background of the Study

mIRC®-triggered malicious web scripts get more rampant these days because of the vulnerability of mIRC® and are getting more annoying to users and to the people maintaining internet cafés and computer laboratories. Mostly affected by malicious web scripts are the administrators, technicians and internet café owners. With this problem on hand, there is also another thing that most users do not know. The users are unaware what these malicious web scripts can do to the computer. One internet café is a good example for the proponents motivation, one of the proponents saw how tedious it was to tell users to avoid these websites before they started chatting. Most of the computers in that café had already been infected and the café is losing a lot of bandwidth every time a user runs in the infected mIRC®,

1.2 Statement of the Problem

The present study seeks to answer the following general problem: How can detection and prevention of mIRC®-triggered Malicious Web Script be done?

Specifically, it seeks to answer the following questions:

- What are the characteristics of a malicious web script?
- How do malicious web scripts contaminate its victim's PC and spread itself over the internet?
- What are the effects of malicious web scripts on a PC?
- What are the types of malicious web scripts?

- What are the different strategies against malicious web scripts?

1.3 Objectives

The general objective of this study is to develop a catching script in mIRC® and a software for detecting and preventing mIRC®-triggered malicious web scripts running in the background.

The specific objectives are:

- To recognize malicious web scripts
- To identify how malicious web scripts contaminate its victim's PC and spread itself
- To identify the effects of malicious web scripts on a victim
- To be familiar with the different strategies against malicious web scripts

1.4 Scope and Limitation

The study focuses on the three types of malicious web scripts: Trojan, Ad-ware, and a combination of the two. The scripts that the proponents be detecting and preventing would be scripts that runs in Windows platform and are stored in the mIRC® folder and in the Internet Temporary folder and not anywhere else. In addition, detection of malicious web scripts is done after it has been downloaded and not upon downloading it. The proponents will also implement a new catching script with software on the background.

The proponents implemented and tested five selected internet cafes and computer laboratories in Davao City. A trace-driven simulation is also done through mIRC® and it shall used to evaluate the new catching script and software and the study is limited within the scope of the specified domain.

1.5 Significance of the Study

This study is significant for all those maintaining internet café's and computer laboratories. Through the catching script that detect and cure any Malicious web scripts; Administrators, technicians and internet café owners will be worry free of any miRC® triggered Malicious web scripts that might infect their PC. In Addition, there will be prevention from contamination of viruses on PC's within internet café's, computer laboratories and at homes with this study. This study can allow users not to disable scripts in the settings of their browsers and worries that may arise upon visiting unknown websites. This would also help them from having hassles in detecting and curing of malicious web scripts.

It is important to use mIRC® as means of catching malicious web scripts since mIRC® is widely used by Filipino chatters and it can be controlled.