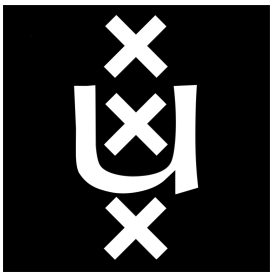
University of Amsterdam
System and Network Engineering
Security of Systems and Networks



Exhaustive Search on URL Shorteners

Alexandros Stavroulakis
Alexandros.Stavroulakis@os3.nl

Xavier Torrent Gorjón
Xavier.TorrentGorjon@os3.nl

Nikolaos Petros Triantafyllidis
Nikolaos.Triantafyllidis@os3.nl

December 9, 2014

Abstract

Our names are Alex, Nick and Xavi and we rule. Alex is the the ruthless ruler. Nick is the handsome hunk. Xavi is the cute little being that we use as a teddy bear.

1 Introduction

This project is gonna change the history of systems security.

1.1 Problem Description

1.2 Previous Work

Most of the previous work which has been done on URL shortening services is based on the use of short URLs and its correlation with SPAM and phishing techniques, whether that is to prevent spamming or to explain how these two are combined. One example of the latter is how the original URL is masked in a way that the receiver of such a malicious email will not be able to realize the fact that by clicking such a link, he or she will not be redirected to a legitimate website.

Another example was the investigation of specific countermeasures take from these particular services to defend against the manipulation of the shortened URLs for malicious purposes; also trying to determine and statistically analyze the extent of spamming given certain geographical locations in which the services were used.

As for the analysis of the URLs as independant links and their respective data, the primary focus was on short URLs collected by popular social media such as Twitter. And the statistics revolved around their popularity lifetimes and the expectancy of the amount of clicks these URLs would get.

After studying our research results and having witnessed what kind of options and possible offensive routes there are available for an attacker to choose from, we have some suggestions