CERIAS

The Center for Education and Research in Information Assurance and Security

DETECTING MALWARE WITHIN OS X SYSTEMS (Work In Progress)

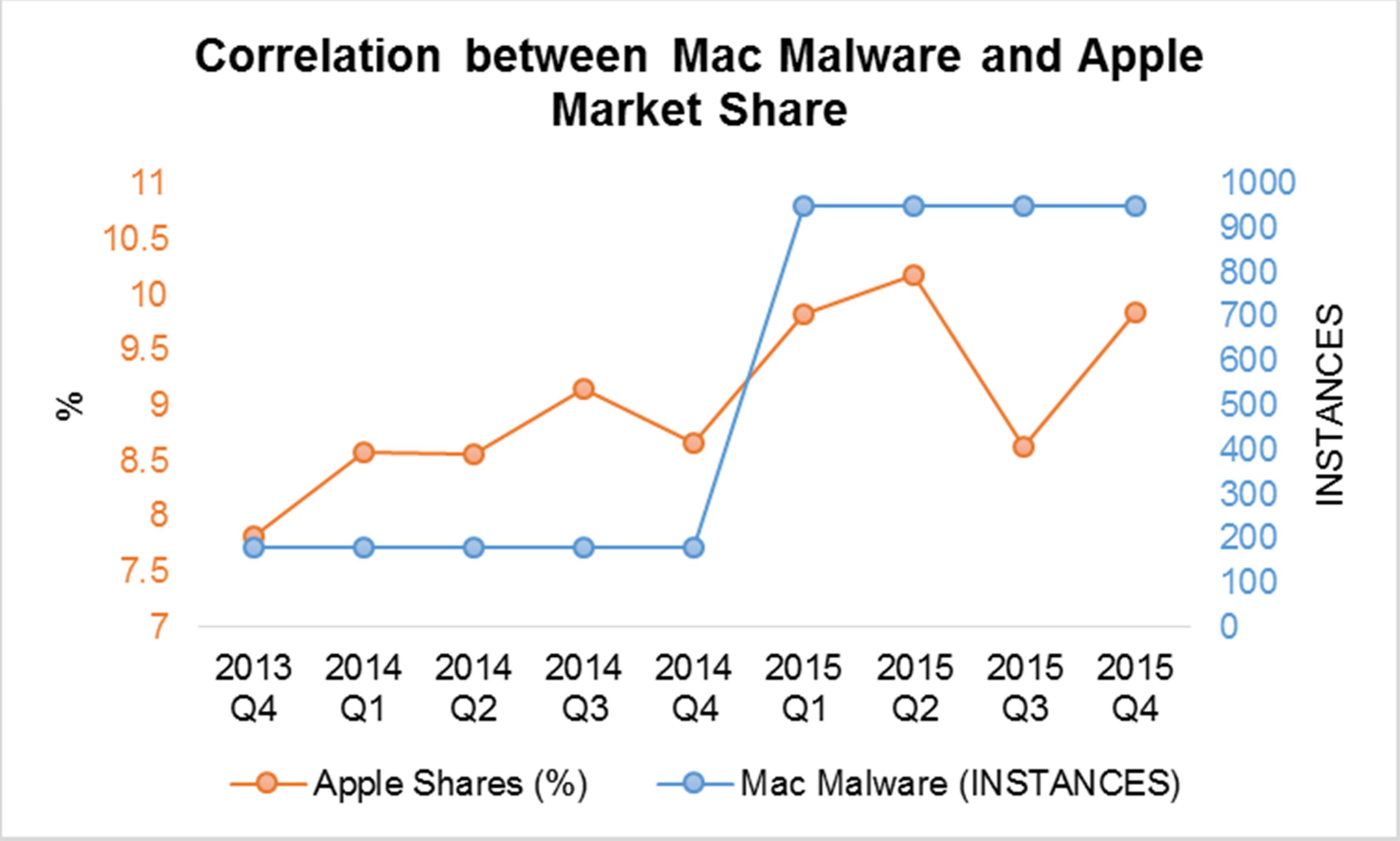
Michael Graham, Prof. Marcus Thompson
Department of Computer and Information Technology
Purdue University

Abstract

Malware is software that is developed with the intent to damage or disable computers and computer systems. The purpose of this poster is to explore the history of Macintosh malware and investigate how it has infiltrated into the Apple OS X environment and the best way for forensics analysts to detect if malware is present on a given machine.

Background

A growing problem that the consumer market is facing today is the development of malware for computers. According to a report released by McAfee Labs in August 2015, it is estimated that nearly 1 million pieces of malware are created every day. Hackers are now starting to target Mac and iOS devices. In recent years, Apple has grown in market share and has even started to branch off into the enterprise area as well. As Apple continues its growth in both the consumer and enterprise markets, its platforms have become a prime target for attackers.



Problem

- Apple market share continues to grow
- Many analysts do not have experience with Macintosh machines
- Malware authors are creating more complex programs for OS X

Methods

- Find source image for current malware
- Infect a newly imaged system with malware
- Obtain forensics image
- Analyze image for traces of infection
- Determine if infection compromises the machine