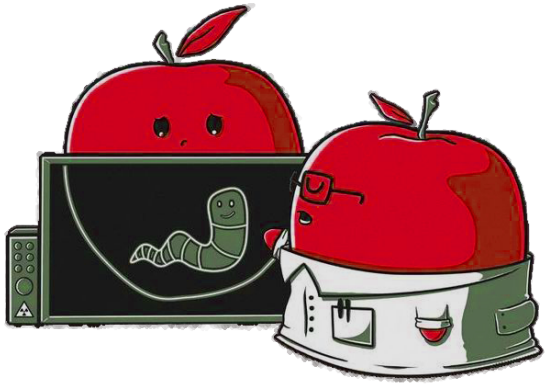
Take a Bite
Finding the Worm in the Apple



Martina Lindorfer, Bernhard Miller, Matthias Neugschwandtner, Christian Platzer
Secure Systems Lab, Vienna University of Technology

Introduction

Is MacDefender Malware a Sign of the Macpocalypse?

By Tony Bradley, PCWorldMay 27, 2011 7:06 AM

More than 600,000 Macs infected with Flashback botnet

by Steven Musil | April 4, 2012 6:25 PM PDT

APPLE '10 YEARS' BEHIND MICROSOFT ON SECURITY: KASPERSKY

Malware
by Steve Evans| 25 April 2012

Welcome to Microsoft's world, Eugene Kaspersky tells Apple

Mac malware Crisis on Mountain Lion eve?

by Paul Ducklin on July 25, 2012 | 10 Comments
FILED UNDER: Apple, Featured, Java, Malware, OS X

Even Apples sometimes have worms in them, admits Cupertino

Sinful humans can drag down even angelic Macs

By Anna Leach, 26th June 2012

Monday, June 25th 2012 at 1:50 pm

Apple No Longer Claims It's Immune to Viruses

By *Eric Limer* ( )

Introduction

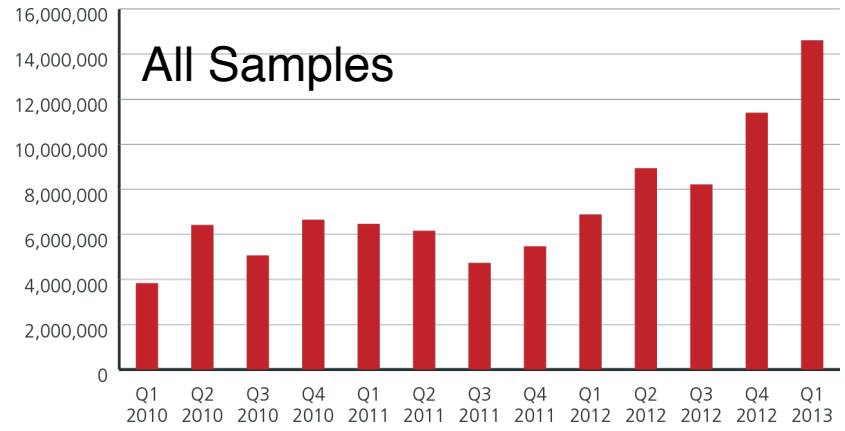
Outline

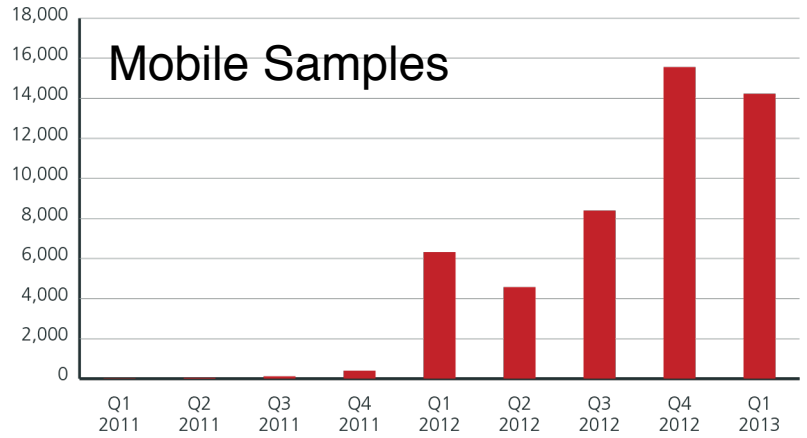
- **Problem Overview**
- iHoneyClient
- Evaluation
- Future Work & Conclusion

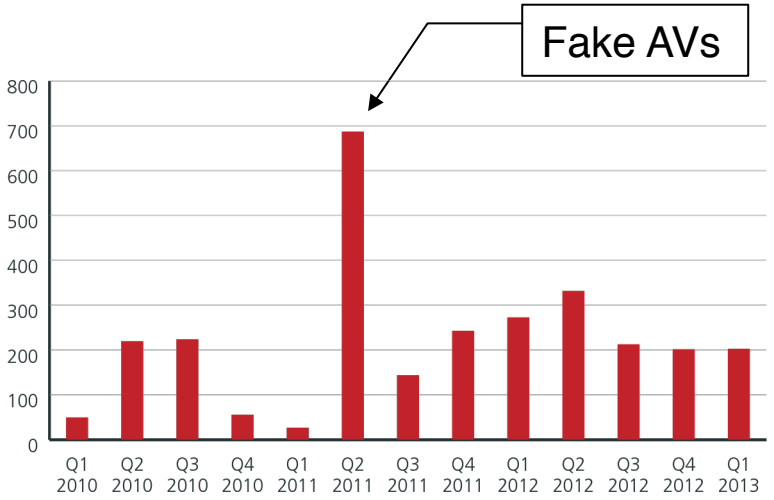
Problem Overview

- Mac OS X reputation of being safe from malware
- Cost-benefit analysis for malware authors
  - Mac OS X currently 9% market share
  - Infection through social engineering (SE):
    Mac users false sense of security?
  - Infection through drive-by downloads:
    Oracle Java, Adobe Flash Player, Adobe Reader
- Several instances of targeted attacks
- Apple slow to react with updates in the past
  - Almost 2 months to fix Java vulnerability targeted by Flashback
- Research in this direction is sparse

New Malware Samples/Quarter







Mac OS X Samples

Source: McAfee Threats Report: First Quarter 2013

Our Motivation

- Anubis: Analyzing Unknown Binaries
  Public Dynamic Malware Analysis System
  https://anubis.iseclab.org

- Windows analysis (since February 2007)
  59,047,857 submissions, 36,885,877 unique files

- Android analysis (since June 2012)
  1,047,366 submissions, 726,853 unique files

- What about Mac OS X?
  How many Mac samples are there in the wild?
  How can we automate their analysis?

Our Approach

- Detection of Mac malware in the wild
  - Crawl known drive-by download sites
  - High-interaction honeypot simulating the whole system
  - Detect successful exploits through created processes & files
  - Record network activity for further exploit analysis

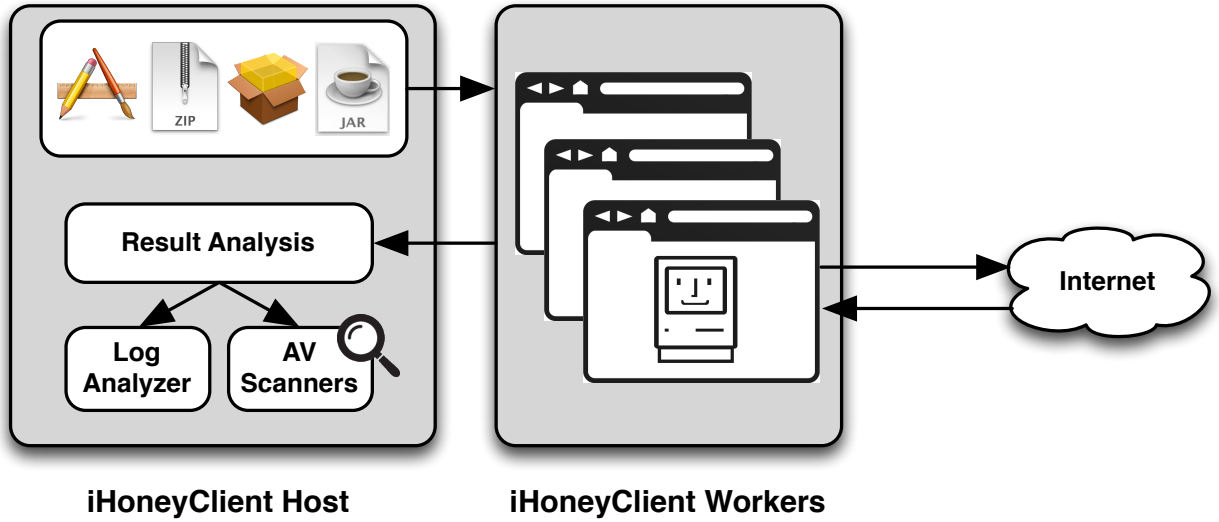
- Dynamic Analysis of Mac malware
  - Execute samples in a controlled environment
  - Record system-level activities (created processes & files)
  - Record network activity

→ VirtualBox-based **iHoneyClient** (honeypot + analysis mode)

Outline

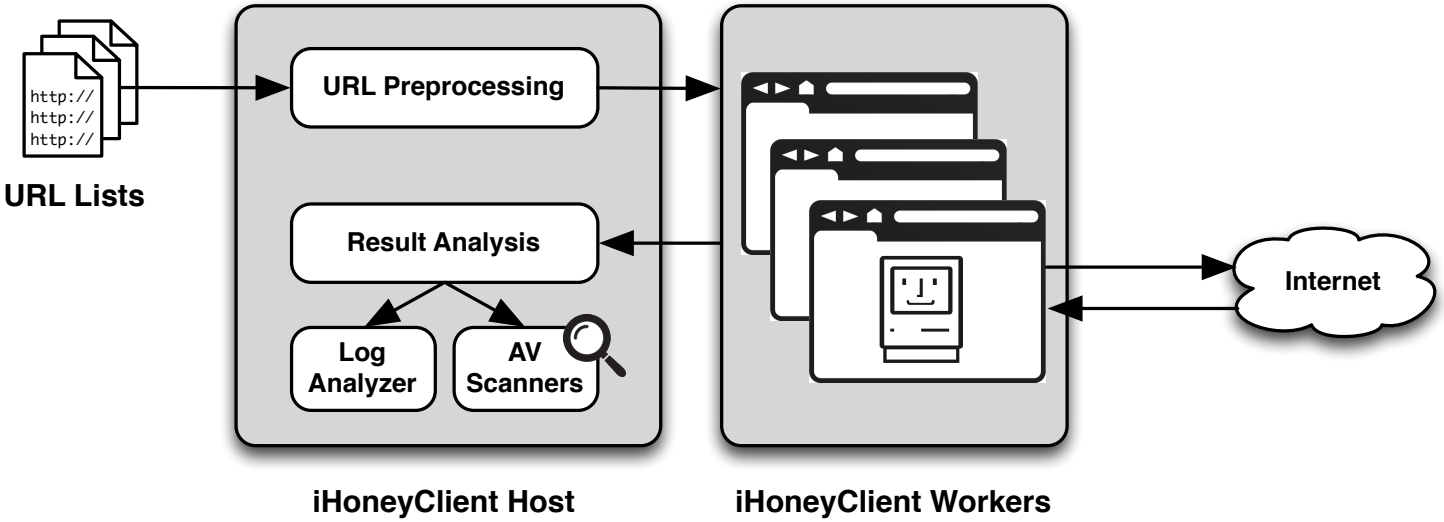
- Problem Overview
- **iHoneyClient**
- Evaluation
- Future Work & Conclusion

iHoneyClient Analysis Mode



- Upload and execute sample to iHoneyClient worker VM
- Logging of all system calls and their arguments
- Monitoring of network activity
- Post-processing to create analysis report

iHoneyClient Honeypot Mode



- Retrieve drive-by download URLs from blacklists
- Preprocess URLs (check availability + content type)
- Visit URL in iHoneyClient worker VM
- Post-processing to detect new infections

Implementation

- System call logging with DTrace
  - Dynamic tracing framework built-in Mac OS X
  - Static and dynamic kernel-level “probes”
  - Probe executes a script to log system call and arguments

- Challenges:
  - Vanilla Mac OS X not fully supported by VirtualBox
    → “Hackintosh” modifications (custom bootloader, kernel module to simulate genuine Apple HW)

  - Process can set P_LNOATTACH flag to disallow tracing
    → Kernel module to prohibit setting this flag

Outline

- Problem Overview
- iHoneyClient
- **Evaluation**
- Future Work & Conclusion

2-Part Evaluation

- Part 1: Evaluation of correct functionality
  - Honeypot mode:
    Detect drive-by download exploits from Metasploit ✓
  - Analysis mode:
    Compare analysis reports with AV threat descriptions ✓

- Part 2: Evaluation on real-world data
  - Honeypot mode:
    Crawl blacklists for drive-by downloads
  - Analysis mode:
    Give overview of current Mac malware behavior

Honeypot Results

- Blacklists for drive-by download sites
  - Malware Patrol
  - Malware Domain List
  - Clean MX
- 6,028 malicious URLs in January 2013
- 2,844 URLs after filtering
- 288 sites malicious JavaScripts
- 5 successful drive-by downloads
  - Dropped 12 different binaries
  - All Windows binaries!
  - But: exploit was successful (cross-platform exploit!)

Analysis Results

- 148 Mac samples from VirusTotal in January 2013

  29% showed any network activity
  - Mainly HTTP, SSL only in 2 samples
  - Only 11% resolve IP through DNS
  - No fallback mechanisms if connection to server failed

  43% performed file modifications
  - Only 6% to LaunchAgent entries (for surviving reboot)

  14% tried to create processes
  - Only 50% of those calls were successful

- Low level of sophistication in examined samples

Outline

- Problem Overview
- iHoneyClient
- Evaluation
- **Future Work & Conclusion**

Future Work

- Perform larger-scale analysis
  - e.g. Google Safe Browsing API
- Investigate cross-platform vulnerabilities and malware
  - Mac “infected” by Windows malware
- Integrate iHoneyClient in public dynamic malware analysis system Anubis

Conclusion

- First to present a dynamic Mac analysis environment
- Also acts as a high-interaction honeypot
- Examined behavior of current Mac malware
- Found little sophistication in existing samples
- Examined > 6,000 URLs for drive-by downloads
- Found no Mac malware in the wild
  - Still successful drive-by downloads (by accident?)
  - No demand (yet) for Mac payloads?
- Results lead us to investigate cross-platform vulnerabilities and malware

Questions?

mlindorfer@iseclab.org
http://www.iseclab.org/people/mlindorfer