The Honeynet

PROJECT

# Client Honeypots
# Its Not Only The Network

Michael A. Davis
Chief Executive Officer
Savid Technologies, Inc.
http://www.savidtech.com

# Agenda

- Who am I?
- What is a Client Honeypot?
- Client Honeypot Techniques
    - Pros and Cons
- The Future
- Questions

# Who am I?

- Michael A. Davis
  - CEO of Savid Technologies
    - Senior Member of the Honeynet Project
  - Published Author
    - Hacking Exposed
    - IT Auditor Magazine, SAGE Magainze
  - Speaker
    - Defcon, CanSecWest, Toorcon
  - Open Source Software Developer
    - Snort-win32
    - Dsniff-win32
    - Ngrap-win32

# What is a Client Honeypot?

- Honeypot
  - Dedicated devices whose value lies in being probed, attacked, and compromised.
- Client Honeypots are the inverse
  - Actively crawl or access the web to search for servers that exploit the client

# Why do we need client honeypots?

- Client Attacks are on the rise (MS)
  - 2005 – 5 Office Vulns
  - 2006 – 24 Office Vulns
- 89% of PC’s infected with spyware (Webroot 2006)
- Identity Theft needs the data on the client
- 4 of the 5 Groups of Windows Top 20 SANS Vulnerabilities are for Client Applications
- Operating System vulnerabilities are decreasing

# Types of Client Honeypots

- High Interaction
  - Integrity Checking/Differential Analysis
  - Drive a browser/client
  - Can find 0-day as well as known exploits
  - Usually requires a VM
- Low Interaction
  - Usually signature based
  - Very fast
  - “wget”

# What can Client Honeypots Detect?

- Application Exploits
- Cross Site Scripting
- Malware delivery
    - Content Analysis
- Depends what you are loooking for

# High Interaction Pros and Cons

- Differential Analysis provides in-depth details
- Can be extended past the browser
  - E-Mail
  - Office Documents
  - Other Client Applications
- Requires a “driver” to run the application
- Expensive to develop

# Low Interaction Pros and Cons

- Simple to build
- Requires signature research
    - Can mitigate by utilizing AV/Spyware detection
    - Intensive
- Very Scalable
- Don’t work well for non browser based applications

# Current Client Honeypots

- Honeyclient
- Microsoft’s Honeymonkey
- HoneyC
- McAfee’s SiteAdvisor

# Honeyclient

- High Interaction
- Proxy based solution
  - HTTP Proxy logs the data
- Perl Script drives IE to site
- After site is visted a long system scan occurs
- Slow
- Parses HTML for more URLs
- Only detects file/registry changes
- Still need a manual analysis
- No Caching/Correlation

# Microsoft's Honeymonkey

- High Interaction
- Used for IE7 Phishing Filter
- Slow
  - Requires the use of many VMs
- Can find 0-day easily
  - Runs URLs on a fully patched machine
- Scans memory as well as file system/registry
- Uses other MS Research projects to help with detection (GhostBuster, GateKeeper)

# HoneyC

- Low Interaction
- Cross Platform (Written in Ruby)
- Uses Snort signatures to analyze data
- Uses Search Engines for URL seed in addition to manually fed
- No Caching/Correlation

# McAfee's SiteAdvisor

- High Interaction
- Very Scalable
- Focus on Data
    - Is the site "bad"
- Utilizes Signatures
- Uses Community to double check (Feedback Loop)
- Utilizes E-Mail as well as URLs and malware

# The Future

- More Client Applications
  - Browsers are not the only target
- More Data
  - StieAdvisor uses the data in one way, what about others?
- Open Community for Data Analysis
  - Tools are not the goal
  - More automated data analysis built-in

# Honeynet Project's Client Honeypot

- Modular
- High Interaction
- Utilizes "low interaction" plugins for data gathering/assessment
- Community to help address data inconsistencies
- Distributed IE Plugin
  - The community can keep data current

# General Architecture

- Follows GenIII Honeynet architecture
- Centralized Collector and Correlator
  - Helps reduce duplicate data
  - Provide URL list to clients
  - Community visits same sites over and over but not new ones
- Client side utilizes kernel level filter to determine exploitation

# Client Architecture

- Kernel Mode Filter Driver
  - Profiles IE a la systrace
  - Functions outside of IE’s profile are examained and recorded
  - Basically a function call list of data
- Similar to a HIPS
  - Instead of alerting/preventing just log

# Problems

- Application profile can be wrong
- Will not catch “in browser” exploits
  - Watch for things that affect the machine’s state
- Not cross platform
  - Is Unix even a client problem?

# Questions?

- Questions?
- E-Mail: mdavis@savidtech.com