The Impact of Honeynets for CSIRTs

18th Annual FIRST Conference
June 28th 2006

DFN-CERT Services GmbH
Jan Kohlrausch and Jochen Schönfelder
Introduction

- DFN-CERT: Computer Emergency Response Team for German research network (DFN).
- Constituency are mainly German universities and research institutes.
Introduction

- Honeypots at the DFN-CERT
  - Participant of the eCSIRT and leurre.com projects.
  - Deployment of nepenthes sensors to capture known malware.
  - Use of sensor networks to collect netflow data.
  - Import and integration of this data into a relational database.
    - Support for incident handling service.
    - Identification of compromised systems.
    - Database allows to find correlations between incidents.
    - Compilation of statistics showing current situation.
Introduction

- Current situation, what we can see:
    - Abuse of bot-networks for DDoS attacks and phishing attacks.
    - Vulnerable systems are identified by massive scanning activity (e.g. class-B networks).
  - Time interval from publication of vulnerability to exploit decreases constantly.
  - Number of zero-day exploits for unknown vulnerabilities increase constantly.
  - Web-browser and common server programs are investigated by black-hats for unknown vulnerabilities.
Introduction

- Current situation, what is **difficult** for us to see at the moment:
  - Selective attacks:
    - Since selective attacks do not leave behind any obvious traces they are in general very difficult to detect.
    - No obvious network activity originates from compromised hosts.
  - Early deployment of zero-day exploits:
    - How to distinguish from known exploits?
    - Early deployment of zero-day exploits is nearly invisible in background noise!
Honeynet Projects

• *Ecsirt* and *leurre.com*
  • Deployment of widespread network of low-interaction honeypots.
    • Malware (e.g. trojans and exploit code) can be automatically captured (by nepenthes sensor).
    • This provides help to track down IRC based bot networks.
  • Compilation of statistics concerning abuse of known vulnerabilities can be done.
Honeynet Projects

• *Ecsirt* and *leurre.com*
  
  • Advantage:
    • Identification of compromised systems:
      • Scanning systems
      • Known internet worms
    • Approaches are very effective concerning known vulnerabilities and non-selective attacks.
  
  • Disadvantage:
    • Detection of selective attacks and zero-day exploits is beyond the scope of these projects!
    • That is the aim of the NoAH project!
NoAH Project

- NoAH: European **Network of Affined Honeypots**.
  - Ongoing research project.
  - Contact to international sites.
  - DFN-CERT will deploy demonstrator.
- Homepage: [http://www.fp6-noah.org](http://www.fp6-noah.org)
- Major aims:
  - Distributed Network of honeypots to detect zero-day exploits and internet worms
  - Generate and disseminate signatures of found vulnerabilities and exploits.
  - Deploy a demonstrator.
NoAH Project

- Hybrid architecture:
  - Deployment of low-interaction as well as high-interaction honeypots.
  - Low-interaction honeypots monitor IP addresses and relay connections to high-interaction honeypots.
  - Design allows to easily deploy low-interaction honeypots in arbitrary networks (e.g. ISP, company, home-user, CSIRT)
- High-interaction honeypots include Argos virtual machine.
Argos:
- Developed at Vrije Universiteit Amsterdam.
- Based on qemu virtual machine.
- Designed to detect exploits for buffer overflow and related vulnerabilities.
  - Tagging of all Network data.
  - Monitor use of tagged data.
  - Raise alert, if
    - Tagged data is executed.
    - Tagged data is loaded into EIP.
    - Tagged data is exclusively used in system call.
NoAH Project

- NoAH's benefits for CSIRTs:
  - Detection of zero-day vulnerabilities
  - Tracking down selective attacks
  - Analysis of unknown exploit code
  - Analysis of potential vulnerabilities

► Helps to identify the attacks and vulnerabilities to keep attention to.
• Detection of zero-day vulnerabilities:
  • Potential to cover a broad range of IP addresses in different networks.
    • Low-interaction components are used as relays to high-interaction honeypots.
    • Integration of CSIRTs, companies, ISPs, and home-users (honey@home) into the NoAH architecture.
  • Argos containment environment allows to generate accurate signatures for vulnerabilities and exploits.
    • Signatures and alerts can be distributed very quickly.
NoAH Project

- Detection of selective attacks:
- Why?
  - Attacker is prepared and motivated to attack the target.
    - Attack will be more sophisticated compared to non-selective attacks.
    - Better chance to detect zero-day exploits.
  - Selective attacks have usually higher impact for the victim.
NoAH Project

• How to attract an attacker?
  • Attractive can be services, position (IP address), DNS name, and bandwidth.
    • Webservice of honeypot can provide (faked) research results or other attractive data (Clifford Stoll's “Cuckoo's Egg”).
    • Honeypot is located in network of company or research institute.
    • DNS name can pretend to be an attractive target (e.g. router, server).
NoAH Project

• How to use NoAH's architecture to track down selective attacks:
  • Low-interaction components (relays) can be easily integrated into arbitrary networks.
  • High-interaction honeypots (e.g. argos) allow to provide real services (web server).
  • NoAH components can be deployed in sensitive networks with acceptable risk for the deploying site.
  • Honeypot data is analyzed at the NoAH core.
    • Deploying sites do not need to spend effort into the analysis.
    • Results are distributed to the affected sites.
NoAH Project

- Analysis of unknown exploit code:
  - Some products exist for monitoring malware at execution time (e.g. norman sandbox).
  - These products do not directly support the analysis of unknown exploit code:
    - Which vulnerability is being exploited?
    - Is the vulnerability already known?
    - Is the exploit working at all?
NoAH Project

• Analysis of unknown exploit code:
  • Exploit code can be analysed and identified using argos:
    • Argos alert indicates successful application.
      • Exploit is detected before it gains control over the attacked machine.
      • Exploit code does not have to be fully working (e.g. due to wrong pointer offset).
    • Exploit can be identified by the corresponding argos signature.
NoAH Project

• Analysis of potential Vulnerabilities:
  • My browser crashes, is this an unknown security problem?
  • Yes, if sensitive memory structures are overwritten by user data.
  • Argos can solve this problem:
    • Deploy the browser in the argos containment environment.
    • If argos raises an alert, a security problem can be expected.
NoAH Project

• Thank you!
• Questions?