Current Threats and the Death of Traditional Defense-In-Depth

Paul Royal
Damballa, Inc

RAID 2008
17 September 2008
Traditional Defense-In-Depth

- What’s used to protect the network?
  - Firewall, IPS/IDS

- What’s used to protect the host?
  - User Access Control
  - AntiVirus

- Host-based AV
  - Uses complex, heuristics-based detection along with signature matching
Traditional DID Cont’d

• **What does current host-based AV buy you?**
  - Nothing

• **Project: ZeroPack**
  - Proof-of-concept obfuscation tool
  - Developed by a research intern working part-time for two weeks
Scaling Up Threats

- **Server-side Polymorphism**
  - Attacks the heart of the traditional host-based AV model by automating mutations

- **When done professionally: Kraken**

![Kraken Unique IPs per day](chart)

File `yy.exe` received on 04.22.2008 03:27:05 (CET)
Current status: `finished`
Result: 6/31 (19.36%)
Threat Landscape Changes

- **Botnets**
  - Getting smaller (harder to detect) with some exceptions (e.g., Storm still 100K+)
  - Increasingly detect instrumentation/VMs, use HTTP for C&C, steal proxy-settings to get out

- **Automated SQL Injection**
  - Danmec/Asprox Bot Malware
    - Used to automatically (and parasitically) build propagation infrastructure

- **Rootkit Trends**
  - Kraken, Storm abandoned rootkit components
  - Less than 35% of malware requires administrator access to function (August 2008)
Alternative Approaches

- Consider each form of visibility (e.g., at network egress, on the host) a "perspective"
  - Any given perspective has an incomplete picture of the threat landscape
- Need a broad, multi-perspective approach for detecting threats
  - Damballa detects compromises in enterprise networks using a combination of
    - Data Mining (e.g., at network egress)
    - Machine Learning (e.g., at network DNS)
    - Malware Analysis (on internal/external malware)
  - Compromise rate for a Global 1000 company (with DID – firewall, AV, IPS/IDS) around 3%-5%