Whitelisting

David Billeter

Vice President, Information Security

InterContinental Hotels Group

June 2010

Attacks

- Common Attack Vectors
  - Malware is being customized
  - Evidence that malware is going through a QA process to avoid detection by major anti-virus systems
  - Malware is being run in shells to prevent detection by anti-virus
  - Common types of antivirus software and logging being turned off

Blacklisting

- Compares incoming data with database of known malware signatures
  - Missing new, complex attacks
  - Signature files growing in size and number
  - Necessary lag time between day zero and protection
  - Balance between speed of reaction and testing
- Widespread implementation
  - Users beginning to turn off anti-virus for performance reasons

IHG
InterContinental Hotels Group

Whitelisting

- Only allows approved programs to run
- Variety of implementation methods
- Real-time whitelisting and point-in-time whitelisting
    - Real-time can prevent attacks
    - Point-in-time involves comparison with “known good state”

IHG
InterContinental Hotels Group

Challenges

- Comprehensive real-time whitelisting difficult to manage
  - Can work well in “locked down” environment
- Integration with system updates
  - Global software issues
  - Need to turn off / update / rescan
- Point in time whitelisting
  - taking full image in known good state
  - later using that to compare to then current state
    - Labor intestive
    - After the attack has been successful

IHG
InterContinental Hotels Group

Strategy

- Blacklisting remains vital
  - Blacklisting and whitelisting should both be used
    - Test thoroughly for conflicts
  - Neither can be achieved perfectly
- Real-time whitelisting
  - Maintain different profiles for various types of systems (i.e. developer desktop vs. executive laptop)
  - Repeatedly test system
    - Blocking specific malware
    - Conflicts with other applications

IHG
InterContinental Hotels Group

Strategy

- Point in time whitelisting
  - Significant manual effort; system administrator involvement
  - Limit to major servers
  - Run a sample on a regular basis
- Move away from thinking in silos
  - Integrate strategy with file integrity monitoring, logging, intrusion detection, and incident response
  - Watch and adapt

IHG
InterContinental Hotels Group

Questions