Intel Botnet Detection and Remediation techniques

David Brockmyer, Intel IT Information Security
May 30, 2012
Legal Notices

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2012, Intel Corporation. All rights reserved.
Intel IT Vital Statistics

6,400 IT employees
54 global sites

91,500 Intel employees†
164 sites, 62 countries

87 Data Centers
~75,000 servers

>142,000 Devices
>109K PCs (80%+ mobile)
>33,000 Handhelds (58% BYO)
Consumerization of IT

**Consumerization**: the increasing influence that our technology experiences in our personal lives, both hardware and applications, have on the technology that we expect to use at work.

**Mobile Business PCs**
- Managed Standard
  - 2-4yr refresh
  - <24 month avg.
  - SSDs as standard
  - BYO models in pilot

**Personal Companion Devices**
- >29k devices, 58% personal
- Broadening list of apps/services
- Abstracting data & apps from devices

**Social Media**
- Internal & external collaboration tool
- 23% employees contribute internally
- Connecting customers globally

**Video Collaboration**
- Integrated range of solutions from large room to PCs
- >600 conferences per week
- $73M avoided in travel in 2011
User Systems

Internet Consumption

Networks

- Mail Gateway
- Proxy
- Botnet Detection

Systems

- Netflow
- NIDS
- Botnet Detection
- Log Monitoring

- AV
- HIPS
- Encrypt
Web Presence

Internet Delivery

Platforms

WAF

3-Tier Arch.

Vuln Scans

Testing

Systems

AV

HIPS

Log Monitoring
Sharing Intel IT Best Practices with the World

Learn More About Intel IT’s Initiatives at www.intel.com/IT
Thank You