

# Information Security Update

John D. Halamka MD  
Chief Information Officer

# The State of the Internet in November 2011

- Studies indicate 48% of internet systems are infected now (worldwide)
- Escalation of malware quality and quantity, began in March-April of 2011 (organized crime now uses internet identity theft as a business)
- A new virus is released every 30 seconds, there is a 400% increase in Android device hacking, and 150000 malware variants are found on the internet at any moment (80% are on legitimate websites)
- Risk exists on all Windows, Mac OS X, and Linux platforms (alas, there is no silver bullet)

# The State of BIDMC

- 14501 total devices on network
- 3353 research, departmental and personal devices are not managed by IT (these are the most often infected)
- 11566 BIDMC user accounts
- 589 Needham user accounts
- 212 Websites or applications with remote access

# The Risk

- Every day users download malware and we eliminate it via early detection, remote access to the device or a visit to the device
- We have much more sophisticated monitoring systems than most hospitals so we can see what is happening
- We have hired numerous industry specialists from McAfee, RSA and Verizon to study our environment.
- Although they have made a few technology suggestions, the major need is policy improvement

# The Risk - Home Computers

Drop Server	200.63.44.172
Finding Type	Corporate Credentials
Description	An authorized user accessed one of the organization's resources, BIDMC Portal, from an infected machine (a screenshot is attached). The Trojan horse captured the credentials.
URL	https://portal.bidmc.org/login.aspx?item=/default&user=extranet\Anonymous&site=website&url=/default.aspx
IP Address	24.63.18.108
Timestamp	Wed, 17 Aug 2011 01:06:01 GMT
Rawtext	<pre>"1856";"TOSHIBA-PC_775A658D6522DF69";"-- default -- ";"33556489";"https://portal.bidmc.org/login.aspx?item=/default&amp;user=extranetAnonymous&amp;site=website&amp;url=/default.aspx";"";"1313543161";"188203365";"- 14400";"#6;#0;?#29; #0;";"1033";"C:Program Files (x86)Internet Exploreriexplore.exe";"Toshiba- PCToshiba";"12";"https://portal.bidmc.org/login.aspx?item=/default&amp;user=extranetAnonymous&amp;site=website&amp;url=/default.aspx Referer: https://portal.bidmc.org/login.aspx?item=/default&amp;user=extranetAnonymous&amp;site=website&amp;url=/default.aspx User input: lxxxxaKxxxxx3 POST data: __EVENTVALIDATION=/wEWBALh8vWcAgKvpuq2CALyveCRDwL jNCfD1D ONbAiUFgkw75ofRC13PVI8NZ <b>username=sxxxxa</b> <b>password=Kxxxxx13</b> LoginButton.x=0 LoginButton.y=0";"24.63.18.108";"US";"1313543148"</pre>

# Mitigation

- Surveillance and Detection
  - Scheduled vulnerability scans of managed devices using Nexpose (IP)
  - Augment internal capability with Dell SecureWorks hosting services (IP)
  - More extensive use of logs to identify and correlate suspicious behavior (C)
- Containment and Cleaning
  - Locking down outbound connection from servers, i.e. “white listing” (IP)
  - More aggressive anti-virus update cycle as released rather than time of day (C)
  - More frequent full scans 3x daily rather than 2x weekly (C)
  - Higher sensitivity settings on scans (C)

# Mitigation

- Prevention
  - Increase Internet content filtering restrictions (F)
  - Reduce/eliminate local administrative rights on workstations and laptops (IP)
  - Introduce McAfee Site Advisor to alert users of web site reputation (F)
  - Stepped up use of Intrusion Protection blocks on web activity (IP)
  - More aggressive updates of Java, Adobe and other high risk apps (IP)
  - Two-factor identification for remote users (F)
  - Isolate FDA regulated devices (F)

# Mitigation

- Metrics and Controls
  - Baseline “risk” level of each subnet
  - Past incidence of malware
  - Extent of local administrative rights
  - Content filtering rules
  - Average Nexpose score
  - Incidence of devices with out-of-date anti-virus files

# Content Management Pilot

- Recommend we apply controls to Renaissance and 109 Brookline (2nd or 3rd floor)
- Determine impact of controls
- Tune as needed
- Rollout to other buildings only after Ops review of data and additional policymaking
- Observe and adjust on continuing basis

# Questions?

- <http://geekdoctor.blogspot.com>