Phishing at your own risk

Jan Vykopal, Jan Soukal

33rd TF-CSIRT meeting, Dublin, Ireland, June 2nd, 2011
• Team of Masaryk University, located in Brno, Czech Republic

• Constituency: ~ 40 000 students, > 4 000 staff

• Four key services:
  • Incident handling
  • Intrusion detection
  • Alerts&warnings, announcements
  • Education and training
Handler's nightmare

- Spear phishing is still growing
- Targeted at people and systems at university (SquirrelMail, Horde)
- Sent from compromised accounts
- (Fortunately) poorly translated to Czech

- Anti-spam and anti-phishing filters are blind:
  - E-mails sent from/to **trusted** domains
  - URL links replaced by forms in attachments
  - Not enough keywords

- User is the **important** link (**weakest** or **strongest**?)
Gone phishin'

- End user education/training
- Voluntary participation (~250 students and staff)
- Subscribed users are exposed to 3 different e-mail traps based on real attacks
- E-mails are sent randomly in 30 days
- User actions are logged and evaluated
- Traps, user score and attack explanation is then presented
Gone phishin': traps

• 1st trap
  • *Generic* phishing: targeted at no existing/specific system or group of users
  • Very poor translation
  • Sent from address *eldorado@bandits.wild.west*

• 2nd trap
  • Targeted at one of the university information systems
  • Carefully crafted mail (proper language, real sender address)
  • No URL in mail, bogus form attached

• 3rd trap
  • Targeted at another university information system used by everyone
  • Carefully crafted mail again, but with URL
  • Typosquatting in use (*mumi.cz* instead of *muni.cz*)
Lessons learned

- Difficult traps were too difficult: users forgot that they had participated in the training
- Immediate vs. ex-post feedback
- Discuss it with admins of ”affected” systems
- Support at faculties (electronic bulletin boards, mailing lists) is essential

- **Game is more attractive than other forms**
- We are not alone – e. g., Wombat Security Technologies
Thank you for attention

**CSIRT-MU** at Masaryk University
Brno, Czech Republic

Official web:  
http://muni.cz/csirt

Educational web (in Czech):  
https://security.ics.muni.cz

Jan Vykopal: vykopal@ics.muni.cz
Jan Soukal: soukal@ics.muni.cz
Extra slide: Traps statistics

First trap (generic phishing e-mail)
- 80% resisted successfully
- 14% followed dangerous link
- 6% revealed credentials

Second trap (carefully crafted e-mail with attachment)
- 68% resisted successfully
- 20% opened dangerous attachment
- 12% revealed credentials
Extra slide: Participants

Structure of participants:
- 66% students
- 24% other staff
- 5% pedagogical staff
- 5% alumni

Students and faculties:
- 43% Faculty of Arts
- 43% Faculty of Informatics
- 4% Faculty of Science
- 4% Faculty of Economics and Administration
- 4% Faculty of Medicine
- 4% Faculty of Social Studies
- 12% Other faculties