K-State IT Security Training

Harvard Townsend
Chief Information Security Officer
harv@k-state.edu

April 13, 2011
K-State Union
HAPPY BIRTHDAY
Tom and Garry!

Why should I care about IT security?

IF MY COMPUTER GETS COMPROMISED, IT ONLY AFFECTS ME, RIGHT?

A recently compromised computer at K-State attacked 69,404,957 computers worldwide.

SINCE NEITHER COULD BE HERE TODAY, YOU COULD WIN THOMAS JEFFERSON'S OR GARRY KASPAROV'S BIRTHDAY PRESENTS

Just guess how long it will take the IP addresses to scroll down the screen.

THE TWO CLOSEST GUESSES WILL WIN!
The Threat is Real

1,089 IT security incidents in 2010

- 3.0 incidents per day
- 459 stolen eID passwords
  - 445 individuals
  - 10 repeat offenders (one 5 times this year, another 4 times over last two years!)
- Three high severity incidents
- 560,518 instances of malware detected by Trend Micro OfficeScan (4,383 per day!!)
- 35,590 instances of spyware detected
- 1 compromised computer on campus scanned over 69 million other computers, trying to break into them
- 83 instances of computers infected with malware that steals financial account information
- 83 DMCA/copyright violation notices
- 20+ stolen laptops
- 10 defaced web sites
Not a good trend!!
K-State IT Security Incidents in 2010

Categories

- 408 Spear phishing
- 355 Spam source
- 344 Unauthorized access
- 103 Malicious code activity
- 93 Policy violation
- 83 DMCA violation
- 23 Criminal activity/investigation
- 10 Web/BBS defacement
- 8 Reconnaissance activity
- 3 Confidential data exposure
- 1 Rogue server/service
- 0 Un-patched vulnerability
- 0 Denial of Service
- 82 No incident

Mostly due to phishing scams (74% of total incidents)
A better trend!
(0.6 -> 0.9 -> 0.6 -> 0.7 per day)
Technology can only do so much...

- **96.5% of the incidents in 2010 attributable to user behavior** (give away password, click on a link, open an email attachment, steal music/movie, …)

- Training therefore important (“There’s no security patch for humans!”)
  - Two “Secure IT” sessions today by Neil Sindicich
  - New employees must complete it within 90 days
  - Working now on next year’s training modules
  - 2,797 have completed the training (1,970 online, 844 in person)
  - Required of students in the fall semester

- Also consider sessions today on “Phishing Scams” and “The Risks of Social Networking”
Fake SSO web page

Real SSO web page
Fake SSO web page – site not secure (http, not https) and hosted in the Netherlands (.nl)

Real SSO web page – note “https”
Result of clicking on eID verification badge on the fake SSO web site, or any site that is not authorized to use the eID and password.

This web site is not authorized to use K-State eIDs

Do NOT enter your K-State eID

Do not enter your K-State eID and password on the previous page. The owner and operator of that web site is not authorized to handle this sensitive information.

Entering your secret information may lead to the operator of that web site fraudulently using your information. If you have entered your eID and password at that web site previously, a good precaution would be to change your password now at the eID web site.

To report an unauthorized site requesting K-State eIDs, send e-mail to webmaster@k-state.edu with the site address.
Result of clicking on eID verification badge on a legitimate K-State web site that is authorized to use the eID and password for authentication
Generic web browsing is dangerous

- Malicious advertisements
  - Entice you to click on the ad
  - Have infiltrated many, many popular web sites

- Drive-by downloads
  - Don’t even have to click on an ad to get infected – just visit the page

- Search Engine Optimization (SEO) poisoning
  - Criminals elevate their malicious sites in search engine results; exploit popular current events
Blackhat SEO Poisoning

Search for “Oscars 2010 winners”

2 of the top 5 search results are malicious pages that infect with FakeAV scareware

Source: Sophos security blog March 8, 2010
Threats in places you wouldn’t normally expect

- Copier/printer/scanner/FAX
  - On the campus network, exposed to the world
  - Have hard drives that store copied documents
  - They run web browsers with default passwords
  - See “Copiers Meet the Network” session for more info

- Digital signage

- Credit card swipe device, Point-of-Sale registers

- Specialized lab equipment

- Gaming devices

- Smartphones (see “Mobile Device Security” session and “Virtual Private Networking” during the lightning round)

- Security cameras

- Environmental control systems
Example of APT – Stuxnet

Advanced
- Used four 0-day exploits (unprecedented)
- 7 methods of replication, including good ol’ USB flash drives
- Used a programmable logic controller (PLC) rootkit
- Digitally signed code with two private keys from stolen digital certificates (from two companies in Taiwan)
- Symantec estimates that the group developing Stuxnet would have consisted of five to ten people and as many as 30, and would have taken six months to develop

Persistent
- Targeted specific Siemens SCADA system manufactured in China… at a facility that was raided by Chinese govt. authorities and equipment/plans confiscated. Hmmm.
- Spread indiscriminately, but only activated when encountered specific SCADA
- Caused physical damage – centrifuges spun fast, then slow, creating vibration that would supposedly destroy themselves while the malware made operation appear normal on the gauges/meters. A cyber attack with kinetic effects

Threat
- Targeted specific system in Iranian uranium processing facility that destroyed 1/5th of their nuclear capability, setting them back several years. Hmmm.
- Many have implicated Israel, others U.S., Russia, or China
For more on this and other new types of malware, see “A Breakdown of Malicious Software” session.
I’m qualified to talk about APT!
You too can be a Certified APT Nerd! (CAPTN)

Announcing the Certified APT Nerd (CAPTN) Credential

I am pleased to announce the new Certified Advanced Persistent Threat Nerd (CAPTN) credential. This certification program is designed for information security professionals looking to demonstrate their proficiency in APT topics.

blog.zeltser.com/post/4408713183/certified-apt-nerd
Other significant incidents

- Stuxnet + ….
- Wikileaks – grassroots cyber activism
  - Interesting social, political, ethical, historical, commercial, military, technical, and security implications
- HB Gary Federal hack… when bragging backfires
  - The case for strong passwords and not re-using passwords in multiple places
  - Are government covert hacking operations blackhat or whitehat?!
- The trust framework of the Internet is undermined – who can you trust?
  - RSA SecurID token-based authentication system hacked
  - Comodo issues SSL certs to a hacker for mail.google.com, www.google.com, login.yahoo.com, login.skype.com
- See session “A Breakdown of Malicious Software” for more information
What’s a feller to do?

If you’re not scared by now, then I’m worried about you and I pity your IT support person.

It’s good to be paranoid!
Before logistics…

Questions/Comments?
Logistics

- Breakout sessions for the morning – two blocks of four sessions each
- Go to any session
- Enjoy refreshments in between sessions
- Lunch on your own 11:30-1:00 p.m. – Network!
- Return at 1:00 p.m. for afternoon sessions, which are a repeat of the morning sessions
- 3:30-4:00 p.m. – return to Big 12 room for wrap-up session
- Powerpoint slides will be available on the event web site soon:

www.k-state.edu/its/security/training/2011-04-13/