



Spring Has Sprung (sorta)!

What's blooming on the horizon?

Harvard Townsend

Kansas State University

Chief Information Security Officer

harv@ksu.edu

2009 IT Security Training Event

April 9, 2009

From a concerned SIRT member:

----- Original Message -----

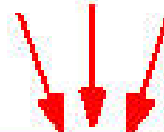
Subject: [CNET News.com](#): Serious security training may benefit from comedy - [CNET News](#)

Date: Wed, 25 Mar 2009 11:32:22 -0700 (PDT)

To: security@ksu.edu

Message from sender:

Interesting take on security training



[Serious security training may benefit from comedy](#) - [CNET News](#)

URL: http://news.cnet.com/8301-1009_3-10203947-83.html

Let's face it, security professionals tend to be pretty techie and the concepts can be complex. How about making it as entertaining as possible?

[CNET](#): The source for computers and technology <http://www.cnet.com>

[Another on the very next day:]

[Agenda]

- IT security incidents at K-State
- Examples challenging incidents
- The changing threat landscape
- What we need to do about it
- And a lot of really bad jokes...

K-State IT Security Incidents in 2007



- 206 security incidents in 2007
 - 0.56 incidents per day
- Severity
 - 6 - High
 - 20 - Medium
 - 180 – Low
- Trend Micro Officescan stats:
 - 12,477 malware instances detected

K-State IT Security Incidents in 2007



■ Categories

- 104 Malicious code activity
- 52 Spam source
- 27 Reconnaissance activity
- 18 Rogue server/service
- 12 Policy violation
- 10 Denial of Service
- 5 DMCA violation
- 5 Criminal activity/investigation
- 4 Unauthorized access
- 4 Web/BBS defacement
- 3 Confidential data exposure
- 0 Un-patched vulnerability
- 5 No incident

K-State IT Security Incidents in 2008



- ~580 security incidents in 2008
 - 1.6 incidents per day
- Severity (531 recorded)
 - 2 - High
 - 20 - Medium
 - 499 - Low
 - 10 - NA
- ~150 spear phishing scams
 - 136 replies with eID/password
- Trend Micro Officescan stats lost in Control Manager upgrade

K-State IT Security Incidents in 2008



■ Categories

- 180 Spam source
- 143 Spear phishing
- 91 Unauthorized access
- 84 Malicious code activity
- 66 Policy violation
- 56 DMCA violation
- 20 Reconnaissance activity
- 16 Web/BBS defacement
- 9 Criminal activity/investigation
- 4 Un-patched vulnerability
- 3 Confidential data exposure
- 3 Rogue server/service
- 1 Denial of Service
- 10 No incident

K-State IT Security Incidents in 2009



- 207 IT security incidents thus far in 2009
 - 2.1 incidents per day
- Severity
 - 2 High
 - 3 Medium
 - 200 Low
 - 2 NA
- Trend Micro Officescan stats:
 - 37,882 instances of malware detected
 - 8,661 instances of spyware detected

K-State IT Security Incidents in 2009



■ Categories

- 77 Spear phishing
- 52 Unauthorized access
- 40 Spam source
- 39 Malicious code activity
- 25 Policy violation
- 17 DMCA violation
- 9 Rogue server/service
- 4 Reconnaissance activity
- 3 Web/BBS defacement
- 3 Confidential data exposure
- 2 Criminal activity/investigation
- 0 Denial of Service
- 0 Un-patched vulnerability
- 2 No incident

[Observations 2007-2009]



- Incidents increasing...maybe (200 – 580 – ~800)
- The threats are real and happening to K-State systems regularly
- Spam consistently a problem
- Dramatic increase in DMCA notices
- Had to create a new category in 2008 (spear phishing)
- DoS less of an issue these days
- Incidents involving confidential data remained the same (3 per year)

[Current Headache]

- Spear phishing scams trying to steal eID passwords to use in Webmail to send spam
- The stats:
 - Frist appeared January 31, 2008
 - 150 in 2008, 76 known versions thus far in 2009
 - 136 replied with their password in 2008, 59 thus far in 2009
 - 44 compromised eIDs used to login to Webmail and send spam thus far in 2009
- The headache:
 - Time-consuming for IT staff
 - Results in K-State being placed on spam block lists by major ISPs
 - Contribute to the worldwide scourge of spam
- Good example of “insider” or the user being a big part of the problem

Demographics of Replies in 2009

- 45 students
 - 6 admitted
 - 11 freshmen
 - 8 sophomore
 - 6 junior
 - 11 senior
 - 5 graduate
 - 1 non-degree
- 2 staff
- 3 faculty
- 3 retired/emeritus
- 2 senior administrators
- 1 group account

[What's different?]

- Not necessarily more incidents, but are definitely more sophisticated and difficult to detect
- Malware *constantly* changing (estimates as high as 50,000 new malware produced daily)
- Escaping detection of Antivirus tools
- WIDE variety of ways to attack

[Vectors for attack]

- Vulnerable operating system (i.e., Windows)
- Vulnerable applications
- Hackers scanning our network from outside or inside the campus network
- Stolen passwords
- USB flash drives
- Malicious web links, even sponsored ads at the top of a Google search
- Web links in an email
- Malicious Facebook ads
- Email attachments
- Extra goodies in P2P downloads
- Instant messaging
- Redirected DNS queries
- Hijacked duplicate web site

[Incident Example #1]

- DNS not working right on several computers
- Packet capture revealed DNS queries redirected to Ukraine, but DNS configuration looked fine
- Fortunately, Ukraine network range already blocked since it was known to be malicious
- Rootkit that's very effective at hiding itself₁₇

[Incident Example #1]

- Prevented security tools from accessing the Internet:
 - Kaspersky AntiVirus
 - Windows Malicious Software Removal Tool
 - SpyBot Search and Destroy
 - Super AntiSpyware
 - STOPZilla
- Acts as DHCP server to give others on LAN bogus DNS information
- Risk is redirecting user to malicious replica of a web site
- Malware known as W32.Tidserv.G

[Incident Example #2]

- Intercepting account information
- Received a report about suspicious traffic to a range of addresses in Latvia
- Netflow analysis revealed 210 K-State IP addresses communicating with this netblock
- Initial packet capture didn't help since communication with Latvia encoded
- Colleague at another univ. cracked the code so Josh could see packet content... bad news
- Malware intercepted HTTP POST requests and sent username/passwords to Latvia, including at least one eID/password pair

[Incident Example #2]

- Executable file hidden in IE browser cache as a GIF file
- Also injects itself in legitimate Windows DLL so that when the DLL is run, so is the malicious code – machine is owned without modifying the registry!!
- Soon blocked the Latvia network range and rebuilt the compromised computers
- Told users to change all their passwords

[Tell more jokes!!]

- A man walks into a bar...
- A horse walks into a bar...
- A jumper cable walks into a bar...

Personal Identity Info Breaches in 2009

- According to the Privacy Rights Clearinghouse Chronology of Data Breaches
www.privacyrights.org/ar/ChronDataBreaches.htm
- Breaches of PII in the U.S. thus far in 2009:
 - 106,911,453 records
 - 178,845 in higher education (**0.17% of total**, or 2.59% if you exclude the 100 million from Heartland Payment Systems)
 - 45 at K-State ☹

Entities involved in 2009 breaches

Heartland Payment Systems
US Army
IRS
FAA
FEMA
Library of Congress
US Consulate in Jerusalem
NY Police Dept
Texas Veteran's Commission
Walgreens
CVS Pharmacies
Comcast
Sprint
Kaiser Permanente

Mass General Hospital
Symantec
Kaspersky
Monster.com
Honeybaked Ham
Pepsi
Continental Airlines
Merrill Lynch
Wyndham Hotels
Los Alamos Labs
State government offices
K-12 school districts
Higher education

[Security Strategy for 2009]

- Policy, policy, and more policy
 - Data classification and security
 - Incident reporting and response
 - Media sanitization and security
 - Audit-driven policies:
 - Physical and environmental security
 - Access controls
 - System development and maintenance
 - Security Communications and Operations

Continue Strengthening Protection of SSNs

- Sweep web sites
- SSN awareness campaign
 - Discover SSNs
 - Get rid of files no longer needed
 - Properly protect those that are needed
- Make Spider (tool that finds SSNs, credit card #s) more widely available
- Implement data classification security standards

[P2P File Sharing]

- Higher Ed Opportunity Act passed in fall 2008 added requirements for dealing with illegal file sharing
 1. Annual disclosure to inform students about illegal sharing of copyrighted materials
 2. “Effectively combat” the unauthorized distribution of copyrighted material.
 3. “to the extent practicable,” offer alternatives to illegal file sharing

Can't Rely Solely on AV Tools

- Characteristics of malware make pattern-based antivirus defense inadequate
 - Malware changes rapidly
 - 50,000 new forms DAILY!
 - Can spread around the world in a matter of hours
- Hackers disable AV software

[More Holistic Approach]

- AV software still has value
 - Use Web Reputation Services and other tools being added
- Strengthen personal firewalls
- Accounts w/o admin privileges
- Promote standard security configurations
- Continue user awareness

[Other Security Projects]

- Laptop whole disk encryption
- Strengthen wireless security (strong encryption and authentication)
- Vulnerability scanning
- Personal digital certificates
- Intrusion Detection System
- Enhanced VPN service
- Evaluate Trend Micro AV for Macs
- Need stronger emphasis on web application security

[Fitting way to end!]

“What’s in a name?”, with apologies to William Shakespeare

- What’s a good name for a man with a shovel on his head?
- How about a man withOUT a shovel on his head?

[What's on your mind?]
