Security (Cont)

Thomas Barrasso

CS-E1 - Fall 2011

Agenda

+ Spam
+ Phishing
+ Malware: Trojans, Viruses, and Worms
+ Hacking & Take Away Points
+ Additional understanding: TEDTalk: Hire the Hackers

Malware

+ Software with a malicious intent.

+ Examples include spyware, adware, viruses, worms, and trojans in the form of keyloggers or rootkits.

+ Accordingly to F-Secure malware is increasing exponentially "As much malware [was] produced in 2007 as in the previous 20 years altogether."

+ Most common form is a trojan.

"I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it's time to go home."

Spam

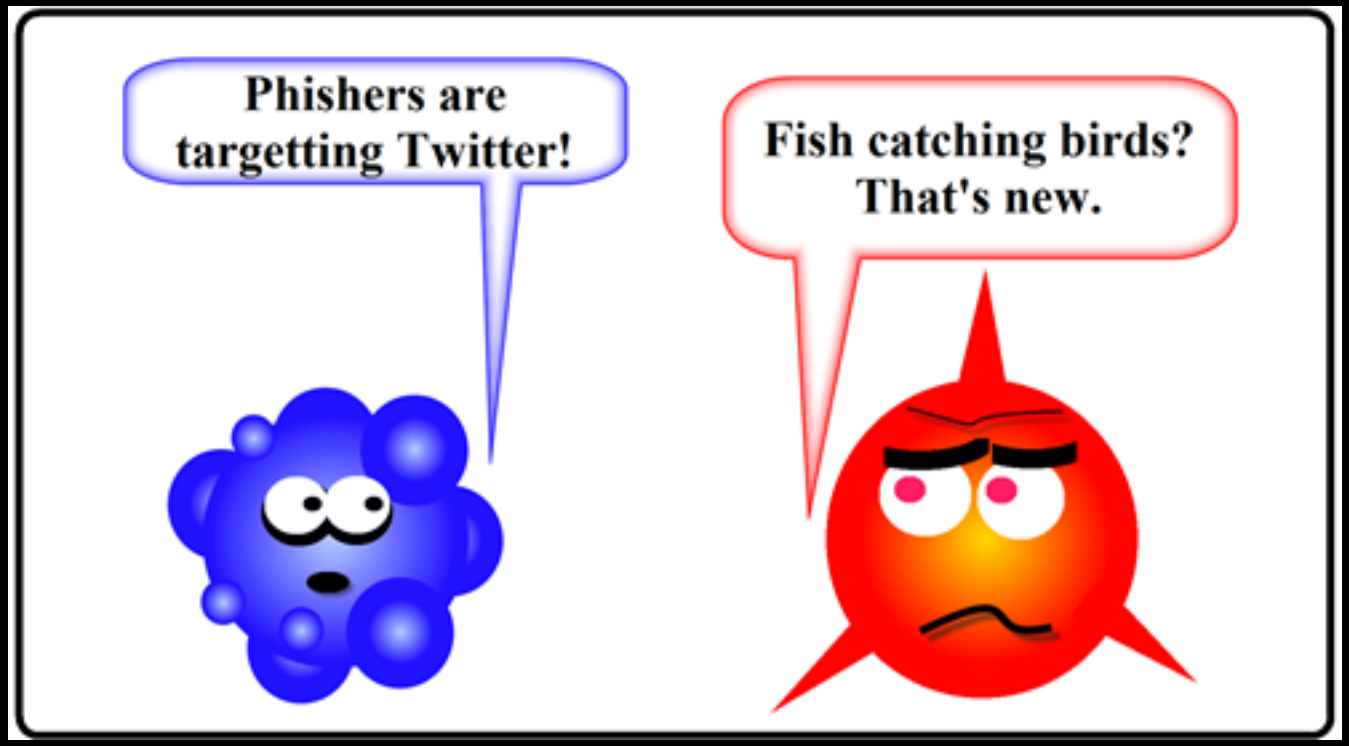
Spam

+ Unsolicited bulk electronic messaging.

+ Over 7 billion spam messages in 2010!

+ Near-zero cost of operation.

+ Spamhaus technical definition: "A message is "spam" if (A) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (B) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent."


Phishers are targetting Twitter!
Fish catching birds? That's new.

Phishing

Phishing

+ Practice based on social engineering designed to appear as another person/ entity with the intent of soliciting personal information.
+ The name hints at its origin, whereby the *phisher* attempts to elicit information using bait, often in the form of an email containing hyper-links or URLs.

+ Do not click on links or copy URLs from an email.

+ Very comprehensive information at justice.gov.

Trojan

+ Derived from Greek mythology during the Trojan War that invited the enemy into secure territory.

+ Designed to appear harmless prior to installation/ execution.

+ BitDefender calculated that in 2009 Trojan-type malware constitutes 83% of global malware making it the most prevalent form.

In The News

+ A Mac OS X Trojan has surfaced through pirated copies of image editing software.

+ Collects personal data and sends it to a remote server, opens ports and communicates with servers, takes screen shots and sends them to servers, and utilizes the system's GPU for mining BitCoins.

+ Lesson: only download software from trusted sources.

+ More info at techspot.com.

Spyware

+ Software that secretly monitors computer activity.

+ Simplest example is a *keylogger* which records keyboard presses and send them to a server.

Adware

+ Computer software designed to play/ display advertisements often in the form of pop-ups.

+ Harmless in and of itself, but often bundled with other forms of malware primarily spyware.

+ Anti-adware software is often not bundled with an operating system for fear of a lawsuit (see *Zango Inc vs. Kaspersky Lab Inc*).

Worm vs. Virus

+ Worms are *self-propagating* and require no user interaction.

+ Does not need to be attached to a particular piece of software.

+ Worms are almost always harmful, minimally consuming bandwidth.

+ Viruses are *self-propagating* but require user interaction.

+ Need to attached to a particular piece of software to self-replicate.

+ Designed to "infect" or modify a file or program to facilitate as a biological virus infects a cell.

Hacking

+ A *hacker* (a person who hacks) often for purposes including profit, protest, or provocation.

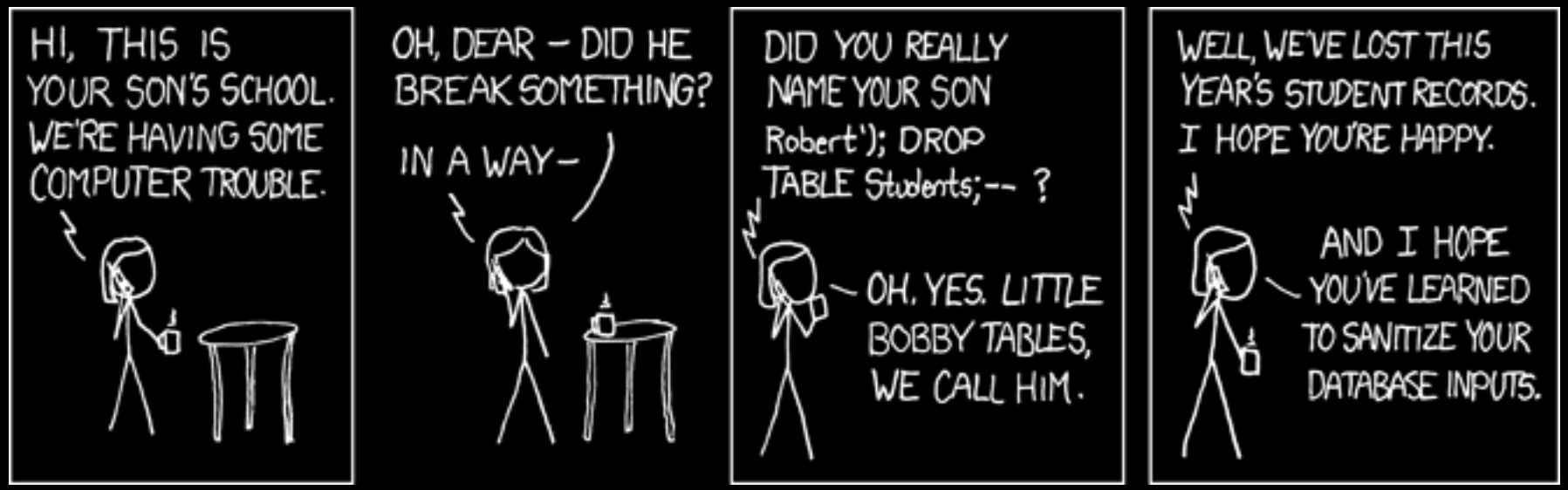
+ Those that hack conducting criminal activity are known as *black hats*, *white hats* when done with noble intention.

+ Often independent computer scientists/ programmers.

+ If you have time check out this great TED Talk called "Hire the Hackers" by Misha Glenny.

Take Away Points

+ Do not click links in an email.
+ Install software only from reputable sources.
+ Only open email attachments from known senders.
+ Update your software (especially web browser) often.
+ Use longer passwords and change them frequently.
+ Very comprehensive information at US-CERT.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

XKCD

fin