

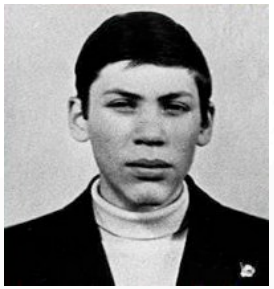

Computer Security

in the news...

Aggelos Kiayias

In the news...

Bank Heist goes Digital



- In summer of '94, Vladimir Levin, a system administrator at St. Petersburg was dialing in into Citibank's cash management system.
  - the system allowed customers to do their own fund transfers with daily turnover of $500 billion.
  - He was allegedly dialing in during peak hours and executing fund transfers that employed significant bank related information.
  - He stole more than $10 million.
  - in August 94, two transfers of $26,800 and $304,000 were flagged as "strange" and FBI got involved.
    - Apprehended in Heathrow, March '95, extradited in '97, got 3 years prison + financial damages.

http://www.byte.com/art/9511/sec3/art11.htm

All around Hacker

Kevin Mitnick

criminal acts :

- Using the Los Angeles bus transfer system to get free rides
- Evading the FBI
- Hacking into DEC system(s) to view VMS source code (DEC reportedly spent $160,000 in cleanup costs)
- Gaining full administrator privileges to an IBM minicomputer at the Computer Learning Center in Los Angeles in order to win a bet
- Hacking Motorola, NEC, Nokia, Sun Microsystems and Fujitsu Siemens systems

During his supervised release, which ended on January 21, 2003, he was initially forbidden to use any communications technology other than a landline telephone

from http://en.wikipedia.org/wiki/Kevin_Mitnick


I will DDoS you

- February 7, 2000, time 10:30 am.
  - Yahoo.com goes down.
  - Incoming traffic in the order of 1GBit/s.
  - CNN, Ebay, Buy.com, Etrade, Amazon follow.
  - Total loss of revenue for yahoo alone over $500,000
  - claims for $1.7 billion overall.
  - In November 7, 2000, 'Mafiaboy' Canadian 15 year old pleads guilty.
    - Janet Reno: *We must punish MafiaBoy*. http://www.wired.com/politics/law/news/2000/04/35765
    - Mafiaboy sentenced to 8 months Youth Detention Center (+$160 fine)


Phish and Chips

- typical case of phishing
  - a week before Christmas, Ms. X notices a wire withdrawal of $1,800 from her bank account.
    - Then, an $800 card charge for escort services.
    - Ms. X had received shortly before two e-mails:
      - One from BankOne asking her to enter some information so that her account was not suspended.
      - Another from Ebay requiring her to enter her account information.
  - She responded to both of them.

    http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18

From: InternetBanking@frostbank.com
Subject: **{SoEspam} New Frost Bank form <message id: 4779523177>**
Date: January 27, 2009 9:12:52 AM EST
To: Aggelos Kiayias <akiayias@engr.uconn.edu>

Dear Frost Bank Customer,

We would like to inform you that we are currently carrying out scheduled maintenance of banking software, that operates customer database for Frost Bank Cash Manager service. Customer database is based on a client-server protocol, so, in order to finish the update procedure, we need customer direct participation. Every Cash Manager Service customer has to complete a Cash Manager Customer Form. In order to access the form, please use the link below. The link is unique for each account holder.

http://treas-mgt.frostbank.com/session50686/rdp/ecomm/frost1/cmform?formid=3161214122630812883842589738165920862956339029535166165 3652347

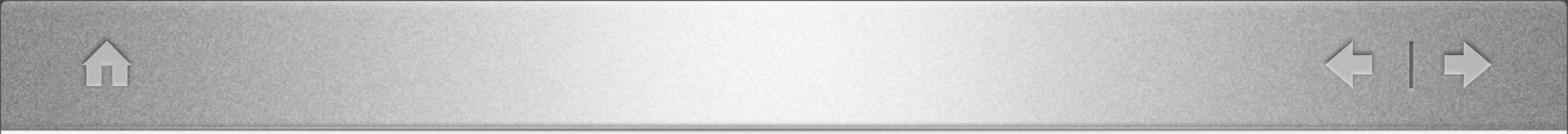
Thank you for your cooperation. We apologize for any inconvenience brought.

Frost Bank Treasury Management

Prevent Fraud.

Frost Bank
Cash Manager Customer Form Version 1.7

http://treas-mgt.frostbank.com.session50686.fddll2.eu/rdp/ecomm/frost1/cmform/?formid=3161214122630812883842589738165920862956339029535166165 3652347



NATIONAL BANK
OF GREECE

Αγαπητέ πελάτη,

τον τραπεζικό λογαριασμό σας έχει αποκλειστεί και θα απενεργοποιηθεί.

Επιβεβαιώστε τον καιρό που θέλετε να συνεχίσετε να χρησιμοποιείτε τον τραπεζικό σας λογαριασμό ή όχι.

Εάν η απάντηση είναι ναι, κατεβάσετε και να συμπληρώσετε το συνημμένο έντυπο.

Εάν η απάντηση είναι όχι, αγνοήστε αυτό το e-mail.

Σημείωση - Μην απαντήσετε σε αυτό το e-mail.

Home NBG Group Retail Business
Contact Us Terms of Use Personal Data Protection


Identity Theft

- A serious concern:
  - in a Federal Trade Commission 2006 ID Theft Report:
    - 8.3 million victims.
    - $15 billion total damage

http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf


Hacked in minutes...

- In a honeypot experiment USAToday and Avantgarde monitored a number of PCs for 2 weeks (Sept. 2004).
- They counted 305,922 break-in attempts.
- The first breach occurred 4 minutes after the test started!
  (against the most vulnerable machine)

http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm


100,000 Zombies

- October 6, 2005: three men are arrested in Holland.
- They allegedly hacked into more than 100,000 computers and turned them into zombies.
- They are accused of blackmailing a U.S. company with a distributed denial of service attack.

http://www.msnbc.msn.com/id/9763824/


Carding anyone?

- Do you want a credit-card?
- How about someone else's credit card?
- you can! it is that easy:
- Find the proper IRC Channel. Type a couple of commands.

```
#MasterCcs 10:00:49 newbie: what i have to type to get cc info ?
#MasterCcs 10:01:15 helper: type !cc
#MasterCcs 10:04:04 newbie: !cc
#MasterCcs 10:05:33 Ccs`: newbie!cc Name: Yukio XXXXXXXX |Address: X-X-X-XXX |
City: Koduru-shi |State: Tokyo |Zip: XXX-XXXX |Phone: N\A
 |Country: Japan |CardType: American Express |Card Number: XXXXXXXXXXXXXXX XXXX
```

Source: the honeynet project. Automated Credit Card Fraud
Dec. 6, 2003


Where do they find all that?

- In June 2005 Cardsystems Solutions, a credit-card processing company in AZ was hacked with targeted malicious intent.
- 40 million debit and credit-card accounts were exposed.
  - Amusingly, their network had been certified in '04 by VISA according to Payment Card Industry Data Security Standard.
  - After the breach it was determined they were not compliant.

http://www.wired.com/news/technology/0,1282,67980,00.html


Santa is coming to town!

- Christmas 2005…
  - one of your "buddies" in your IM service sends you and a nice link for you to go and see Santa Claus!
- You get redirected and you receive your
  - "gift.com"
  - Once executed:
    - Your PC acquires a "backdoor" and is susceptible to various external manipulations --- e.g., keylogging !!

ICSA virus prevalence survey

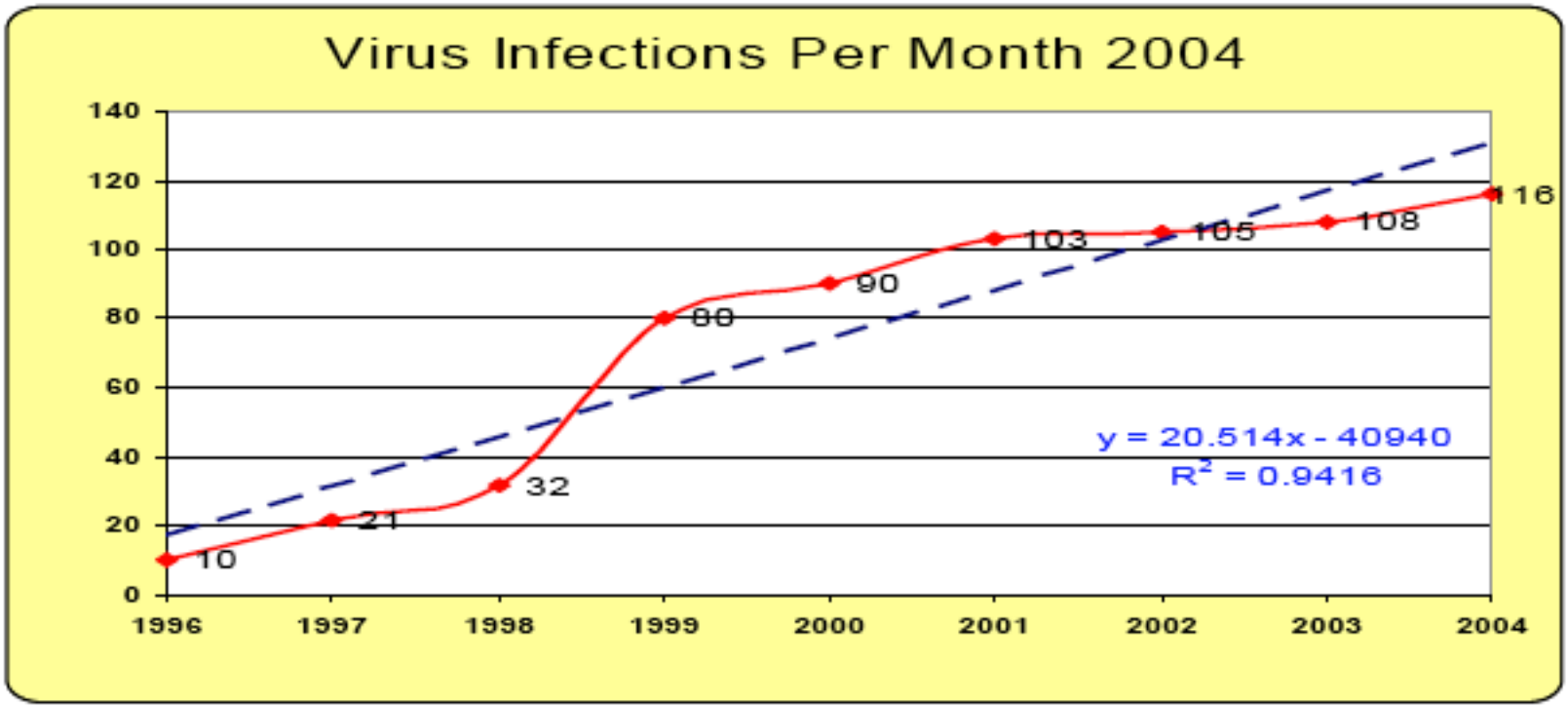


Figure 1: Infections per 1,000 PCs per month

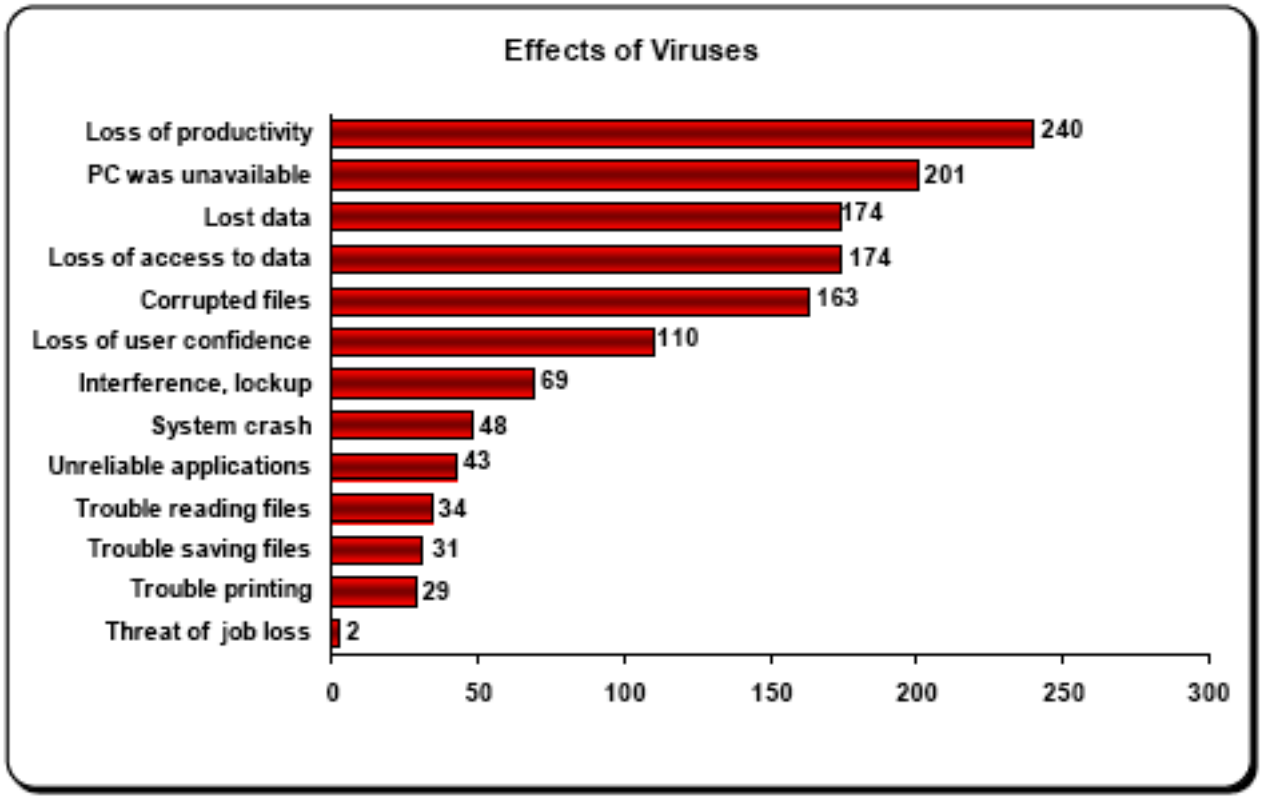

ICSA virus prevalence study

question:
what was the estimated cost in $$$ for all costs in your company's latest virus disaster.

Cost	Frequency	%
$2,500	1	1%
$3,000	3	3%
$5,000	5	5%
$10,000	11	12%
$20,000	9	10%
$30,000	12	13%
$40,000	13	14%
$50,000	10	11%
$100,000	8	9%
$200,000	7	8%
$300,000	3	3%
$400,000	2	2%
$500,000	2	2%
$1,000,000	4	4%
>$1,000,000	3	3%

Table 4: Frequency distribution of dollar costs

ICSA virus prevalence study



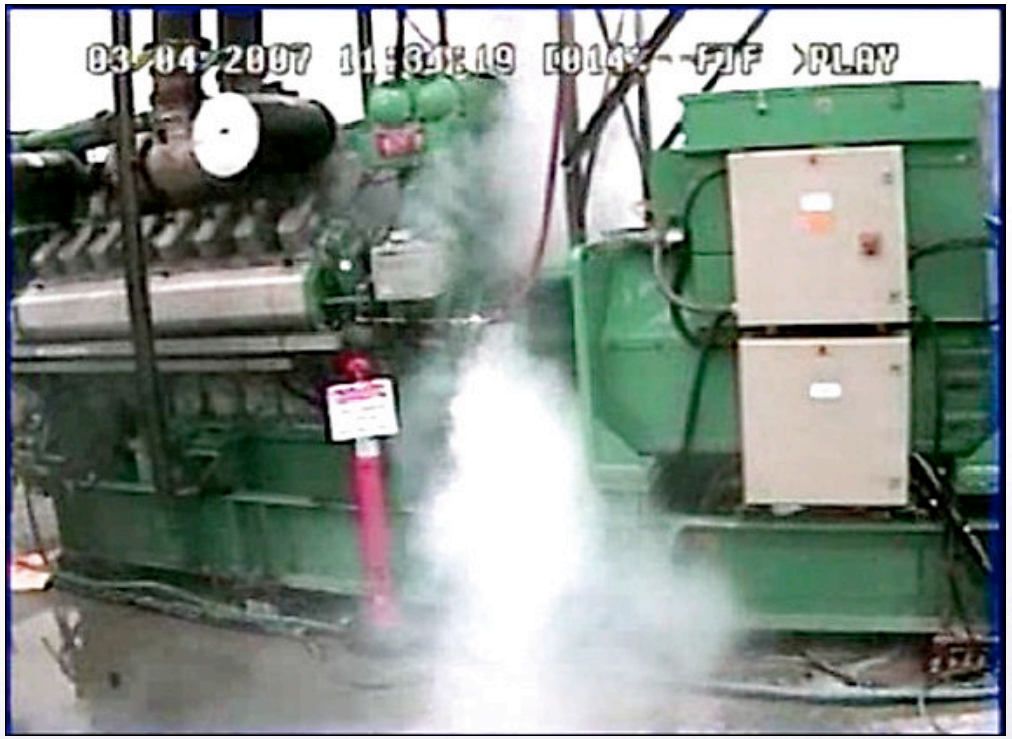
number of responses

Difficulty in security statistics

Infrastructure Attacks

The "aurora generator test"

- In simulation: Remote hacker destroys a $1M diesel-electric generator part of US utility infrastructure



Generator room at the Idaho National Laboratory was remote accessed by a hacker and a $1 Million diesel-electric generator destroyed. (U.S. Homeland Security photo)


2005...

- in 2005, the treasury department was reporting: Cybercrime has outgrown illegal drug sales!

http://money.cnn.com/2005/12/29/technology/computer_security/index.htm?cnn=yes


2006...

- year of spam
  - in oct. more than 90% of all e-mail was junk mail.
- 3-4 million "bots" active at any time in the Internet.
- Attacks have moved from weekends to 9-5 weekdays:
  - online crime is evolving into a full-time profession!

http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html


2007...

- A year of multiple data privacy breaches..
- Millions of private records are revealed to hackers.
- Average annual losses $350,000

http://www.computerworlduk.com/management/security/data-control/in-depth/index.cfm?articleid=1065
http://www.darkreading.com/document.asp?doc_id=133658


2008-9

- Big botnet years :
  - Top botnets: Bobax, Storm, Kraken, Conficker...
  - Conficker 10 million PCs to 2009.
    --- In 12 hours a single bot sent 42,298 spam e-mails.

- Botnets become hard to penetrate, self-protecting, self-healing.


Twitter hacks

January 6, 2009

An 18-year-old hacker with a history of celebrity pranks has admitted to Monday's hijacking of multiple high-profile Twitter accounts, including President-Elect Barack Obama's, and the official feed for Fox News.

The hacker, who goes by the handle GMZ, told Threat Level on Tuesday he gained entry to Twitter's administrative control panel by pointing an automated password-guesser at a popular user's account. The user turned out to be a member of Twitter's support staff, who'd chosen the weak password "happiness."

Cracking the site was easy, because **Twitter allowed an unlimited number of rapid-fire log-in attempts**.

... A fake message sent to followers of the Fox News Twitter feed announced that Fox host Bill O'Reilly "is gay,"

http://blog.wired.com/27bstroke6/2009/01/professed-twitt.html


Passwords?

from a myspace phishing attack

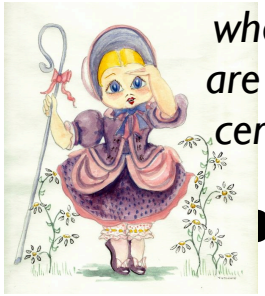
1-4	0.82 percent
5	1.1 percent
6	15 percent
7	23 percent
8	25 percent
9	17 percent
10	13 percent
11	2.7 percent
12	0.93 percent
13-32	0.93 percent

- The top 20 passwords are (in order): password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey

http://www.schneier.com/blog/archives/2006/12/realworld_passw.html


2010

- Increasing privacy concerns for social networking sites such as facebook.
- Cryptographic techniques used for “insurance” + cyberwarfare. the wikileaks case .
- Stuxnet worm : first worm to infiltrate successfully nuclear power plant (in Iran) written with apparent intend to do so. The worm affects the way attached motors to control equipment rotate. In November, Ahmadinejad admitted damage due to the worm.



2011

- Fraudulent digital certificates are created by hackers due to the Comodo and DigiNotar breach (certification authority - CA). CA's are the trusted parties of all Internet transactions they should be unhackable!

40M tokens revoked

- Spear Phishing against RSA: An Excel spreadsheet opened, which was completely blank except for an "X" that appeared in the first box of the spreadsheet. The "X" was the only visible sign that there was an embedded Flash exploit in the spreadsheet. When the spreadsheet opened, Excel triggered the Flash exploit to activate, which then dropped the backdoor -- in this case a backdoor known as Poison Ivy -- onto the system.

  http://www.schneier.com/blog/archives/2011/08/details_of_the.html

- Sony Playstation network hacked - around 100 million users' private data exposed.


2012

- SOPA/PIPA demonstrations : wikipedia blackout Jan 18, 2012.
- ?


End of compsec in the news..

- have a good semester! (and patch your PC before you go to bed tonight...)