CSCE 465 Computer & Network Security

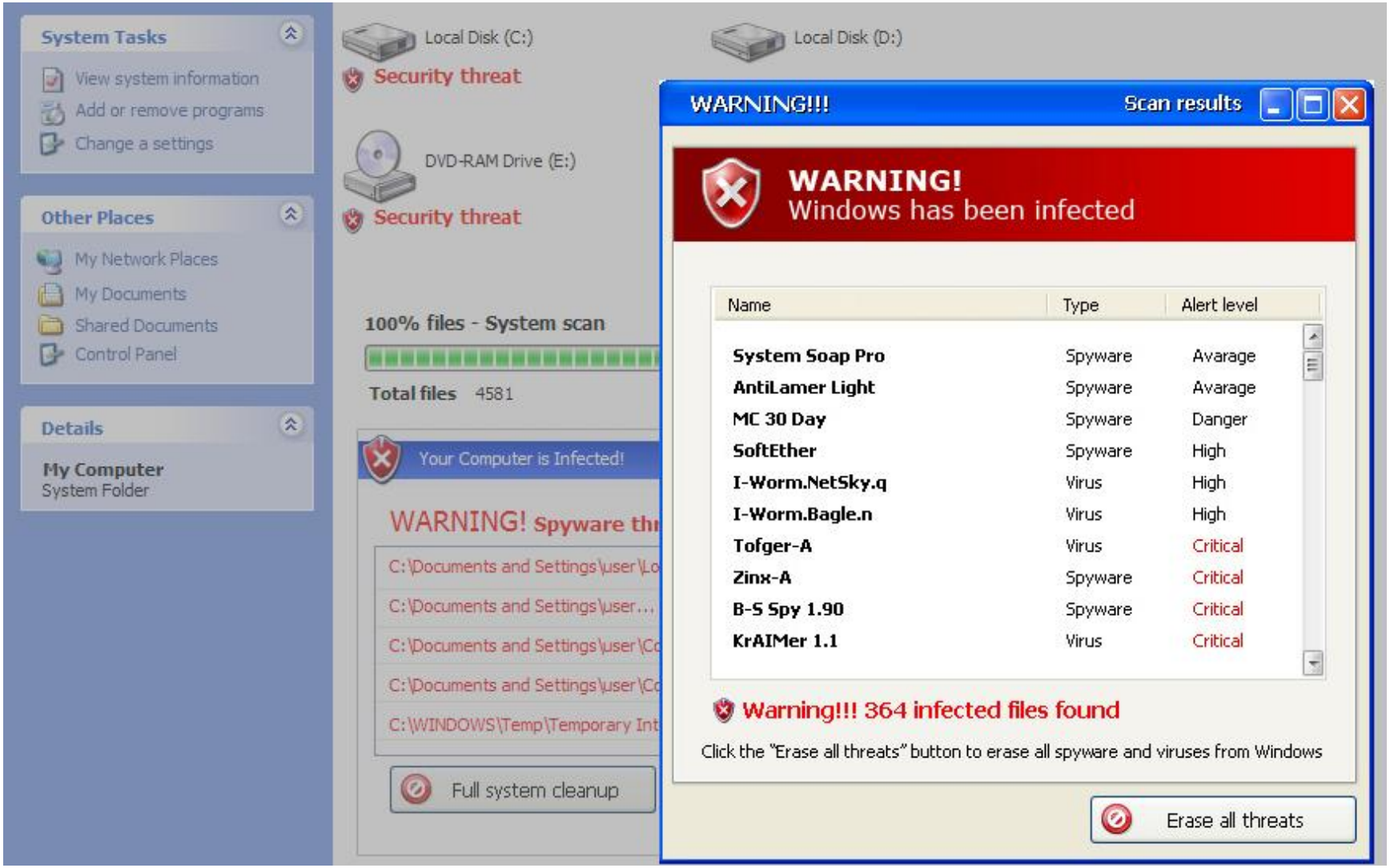
Instructor: Abner Mendoza, Sungmin Kevin Hong

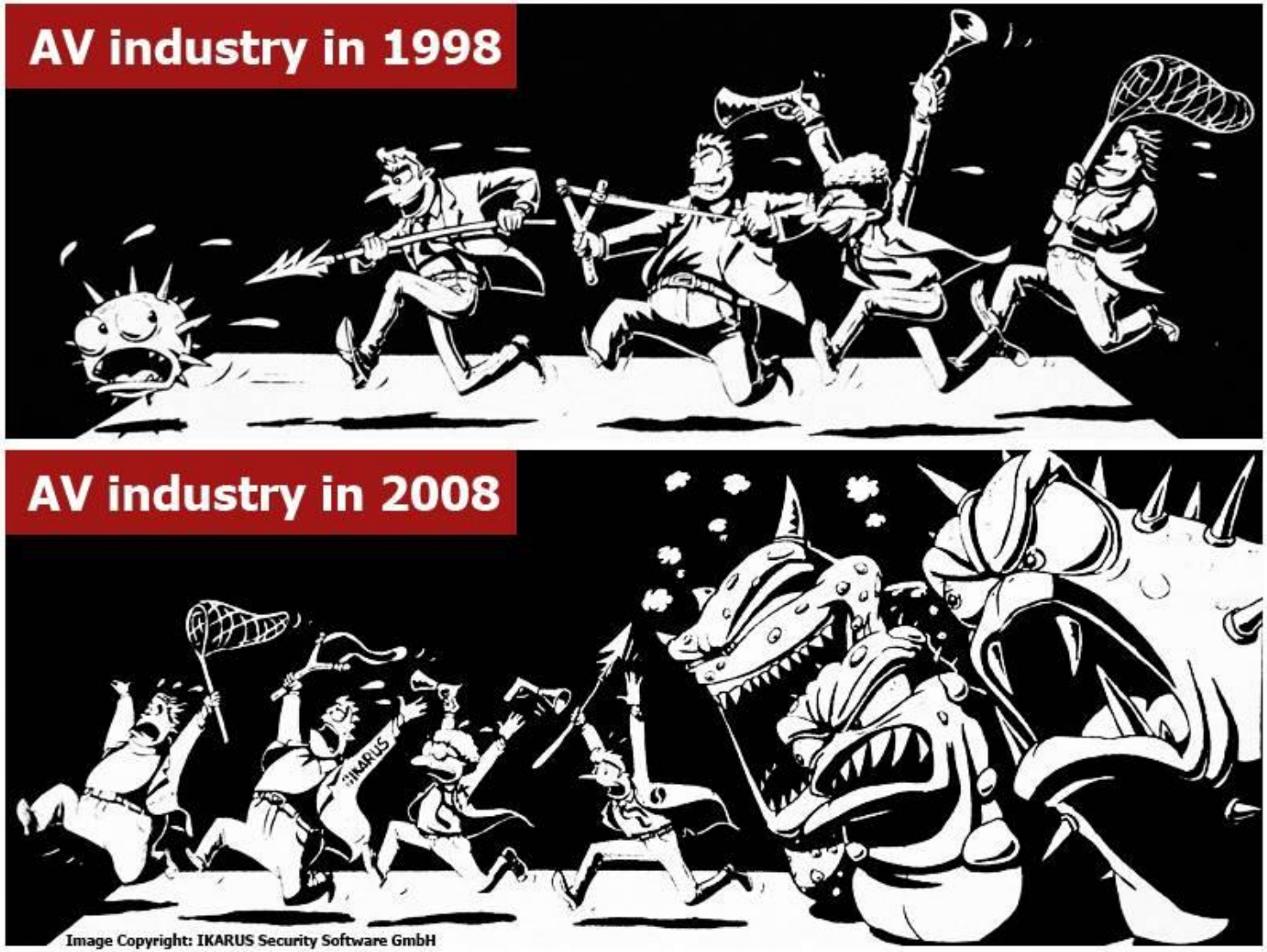
Section 500: http://people.tamu.edu/~abmendoza/csce465/
Section 501: http://people.tamu.edu/~ghitsh/csce465/

Course Logistics and Topics


SECURITY
RISK
HOW SAFE IS YOUR
COMPUTER?


IS IT SAFE?


System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
Local Disk (C:)
Security threat
Local Disk (D:)
DVD-RAM Drive (E:)
Security threat
100% files - System scan
Total files 4581
Your Computer is Infected!
WARNING! Spyware th
C:\Documents and Settings\user\Lo
C:\Documents and Settings\user...
C:\Documents and Settings\user\Co
C:\Documents and Settings\user\Co
C:\WINDOWS\Temp\Temporary Int
Full system cleanup
WARNING!!!
Scan results
WARNING!
Windows has been infected
Name
Type
Alert level
System Soap Pro
Spyware
Avarage
AntiLamer Light
Spyware
Avarage
MC 30 Day
Spyware
Danger
SoftEther
Spyware
High
I-Worm.NetSky.q
Virus
High
I-Worm.Bagle.n
Virus
High
Tofger-A
Virus
Critical
Zinx-A
Spyware
Critical
B-S Spy 1.90
Spyware
Critical
KrAIMer 1.1
Virus
Critical
Warning!!! 364 infected files found
Click the "Erase all threats" button to erase all spyware and viruses from Windows
Erase all threats


AV industry in 1998
AV industry in 2008
IKARUS
Image Copyright: IKARUS Security Software GmbH

Class Question

How would you define SECURITY?

What is Security?

- [Informally] Security is the *prevention* of certain types of *intentional* actions from occurring

  - These potential actions are **threats**
  - Threats that are carried out are **attacks**
  - Intentional attacks are carried out by an **attacker**
  - Objects of attacks are **assets**

Goals of Security

Prevention

- Prevent attackers from violating security policy

Detection

- Detect attackers' violation of security policy

Recovery

- Stop attack, assess and repair damage

Survivability

- Continue to function correctly even if attack succeeds

Components of Security

Confidentiality

- Keeping data and resources hidden/confidential

Integrity

- Preventing unauthorized changes to data or resources
  - Data integrity (integrity)
  - Origin integrity (authentication)

Availability

- Enabling access to data and resources

Why This Course?

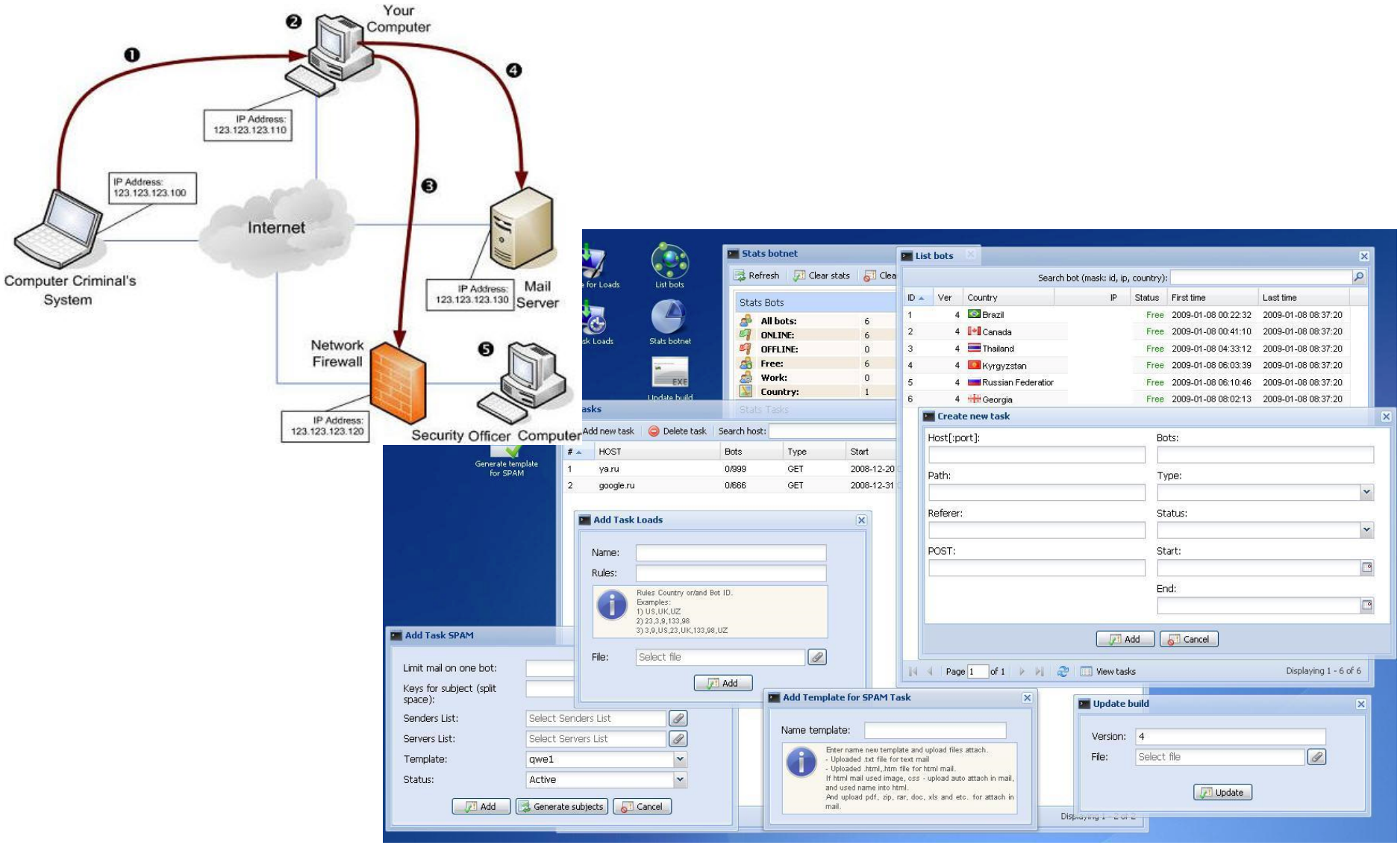
- Increased volume of security incidents
- Security threats
  - Malware: Virus, worm, spyware
  - Spam
  - Botnet
  - DDoS attacks
  - Phishing
  - Mobile (Android/iOS) Malware
  - IoT compromise

Malware

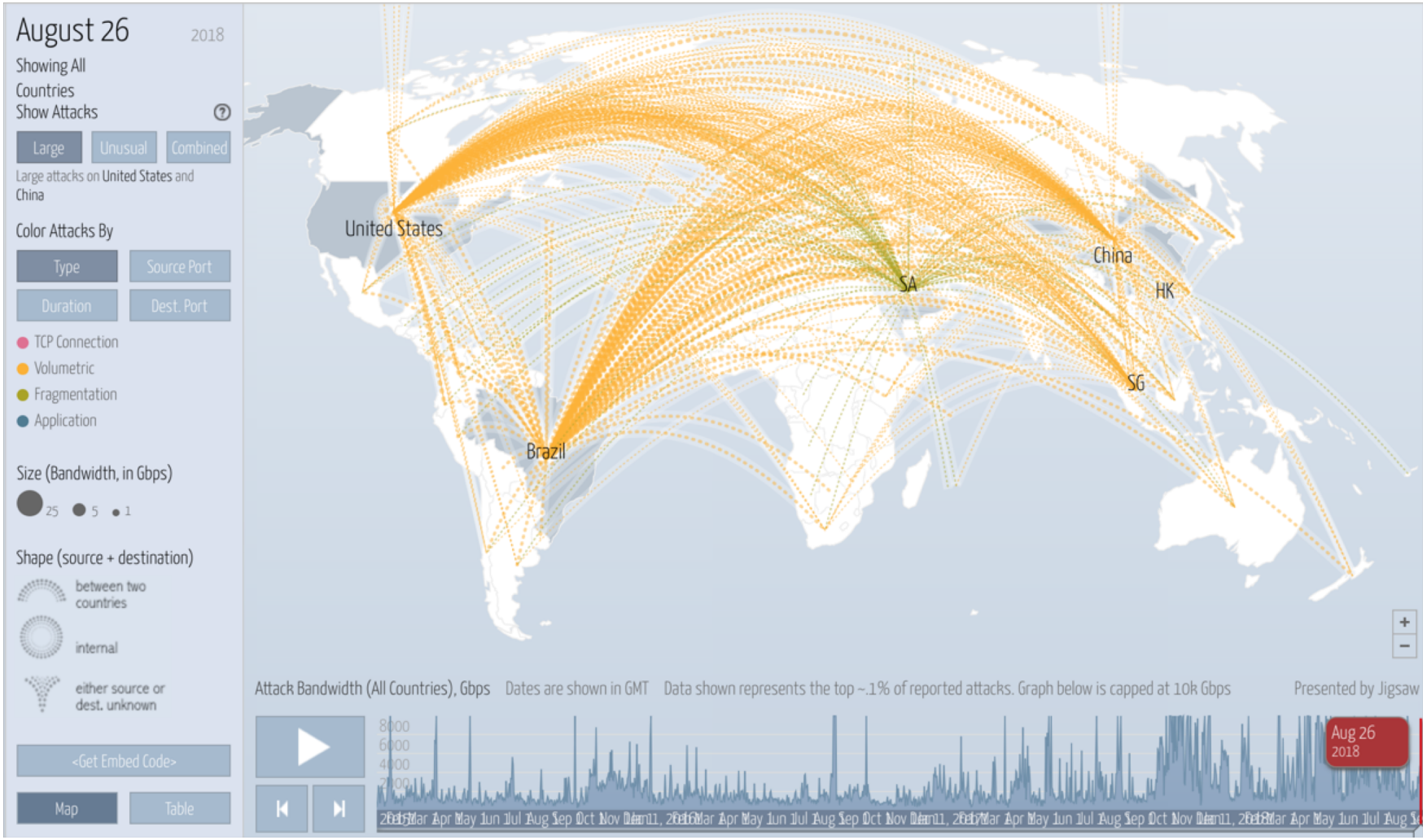

Hijackers
Malware
CWS!
Spyware
Adware


Spyware:
it's not what every well-dressed spy is wearing
Spy-wear

Advanced Malware: Botnet



Consequences: Denial of Service



More…

- “Attack of the tweets: Major Twitter Flaw Exposed” – UK researcher says vulnerability in Twitter API lets an attacker take over a victim’s account – with a tweet. Aug 27, 2009 [Darkreading]
- Conficker worm

- Stuxnet …

Class Question

- Why are you taking this class? Your understanding and expectation?...

Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in information security.
  - Security goals and threats to networking infrastructure and applications.
  - Network security
  - System security
  - Introduction to cryptography.
- Be able to determine appropriate mechanisms for protecting computer &network systems.

Course Styles

- Descriptive: what is out there.
- Critical: what is wrong with ...
- Skill oriented: homework/labs.
  - Explore!
- Interactive: discussion and questions encouraged and considered in grade
  - Students are encouraged to present their findings
- Information sharing: home page, eCampus and email

Course Outline

- Background
  - Confidentiality, integrity, availability
  - Security policies, security mechanisms, assurance
- Network and system security
  - Fundamental security theories, Access control
  - Program/software security
  - Malware
  - Vulnerability analysis
  - Firewalls
  - Intrusion detection

Course Outline - Cont'd

- Cryptography
  - Secret key cryptography
  - Hashes and message digests
  - Public key cryptography
- More
  - Authentication and security handshakes pitfalls
  - IP security
  - Web security

Prerequisites

- CSCE 313: Introduction to Computer Systems
- Programming experience in C/C++ is required
- Knowledge in data communication and networking is required
- Other basic knowledge: operating systems, discrete mathematics…
- The **right** motivations!

Textbooks and References

- Required textbooks
  - [Bishop] Matt Bishop, *Introduction to Computer Security*, Addison-Wesley, 2004. ISBN 0-321-24744-2.
    - *This book contains computer security theory & technologies and will be used for the first half of the course*
  - *[KPS] Network security: PRIVATE communication in a PUBLIC world* by Kaufman, Perlman, and Speciner.
    - This book is very comprehensive in crypto. I will follow it as much as possible for the second half of the course
  - Accessible online through campus library links (choose SAFARI database)
- Reference text(s) and class notes - see web site.

Course Resources

- WWW page:

  Abner: http://people.tamu.edu/~abmendoza/csce465/

  Kevin: http://people.tamu.edu/~ghitsh/csce465/

  – For course materials, e.g., lecture slides, related homework supplements, class notes, tools, etc.

  – Will be updated frequently. So check frequently.

- eCampus (for discussion/Q&A and assignment submission/distribution)

  – You will be automatically enrolled

- Office hour and TA: see course website

Grading

- Grading: Assignments 50%, Midterm Exam 20%, Final Exam 25%, Course attendance 5%
  - There will be some bonus points in homework/labs
- Assignments: Five homework assignments, each including paper-and-pencil questions and/or programming/lab problems.
- Grade scale: 90-100 = A. 80-89 = B. 70-79 = C. 60-69 = D. Below 60 = F
- Late homework will be accepted with a 20% reduction in grade for each day late by
- After grades distributed/returned, 1 week for regrading.

Homework & Labs

- You need both theory and practice
- Labs included in homework: (Tentative list)
  - Packet sniffing and spoofing
  - Buffer overflow
  - TCP/UDP attacks
  - Secret-key cryptography
  - ……
- Mechanism
  - Virtual machine & network using **Texas Cyber Range**
- Many labs are difficult and time-consuming (but very rewarding)
- You are encouraged to work in teams (collaborate, but homework reports should be individual!)
- You are expected to explore issues beyond what's included in lectures by yourselves
- By taking this course, you agree you will not misuse tools obtained in the labs

Ethics & Academic Integrity

- We will study/discuss threats and attacks in the class/lab. You should be fully aware of ethics when studying these techniques. If in any context you are not sure about where to draw the line, come talk to me first.
- The university, college, and department policies against academic dishonesty will be strictly enforced.
- "An Aggie does not lie, cheat, or steal or tolerate those who do."

Next Class...

- Fundamentals of Security
- Theory, Definitions, etc.