Information Security

Sandeep Mudalkar
Founder & CEO of Sytech Labs &
Cyber Crime Investigator/Consultant
Hyderabad.

Viruses, Bots, and Phish, Oh My!

- **What is Information Security?**
- **Why is it Important?**
- **What Can We Do?**

Viruses, Bots, and Phish, Oh My!

What Is Information Security?

- Deals with several different "trust" aspects of information and its protection
- The U.S. Government's National Information Assurance Glossary defines **INFOSEC** as:

> *"Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats."*

Viruses, Bots, and Phish, Oh My!

What Is Information Security?

- Three widely accepted elements or areas of focus (referred to as the "CIA Triad"):
  - Confidentiality
  - Integrity
  - Availability (Recoverability)
- Includes Physical Security as well as Electronic

Definitions

Malware:

- Hostile, intrusive, or annoying software or program code ("maliciousHostile, intrusive, or annoying software or program code ("malicious" + "software“)
- Includes computer viruses, worms, trojan horses, bots, spyware, adware, etc
- Software is considered malware based on the intent of the creator rather than any particular features

Definitions

Internet bot:

- also known as **web robots**, are automated internet applications controlled by software agents
- These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a humanlike manner (i.e., computer game bot)
- Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes.
- Botnet - a network of "zombie" computers used to do automated tasks such as spamming or reversing spamming

Definitions

Adware:

- **Advertising-supported software** is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- Adware is software integrated into or bundled with a program, typically as a way to recover programming development costs through advertising income

Definitions

Spyware:

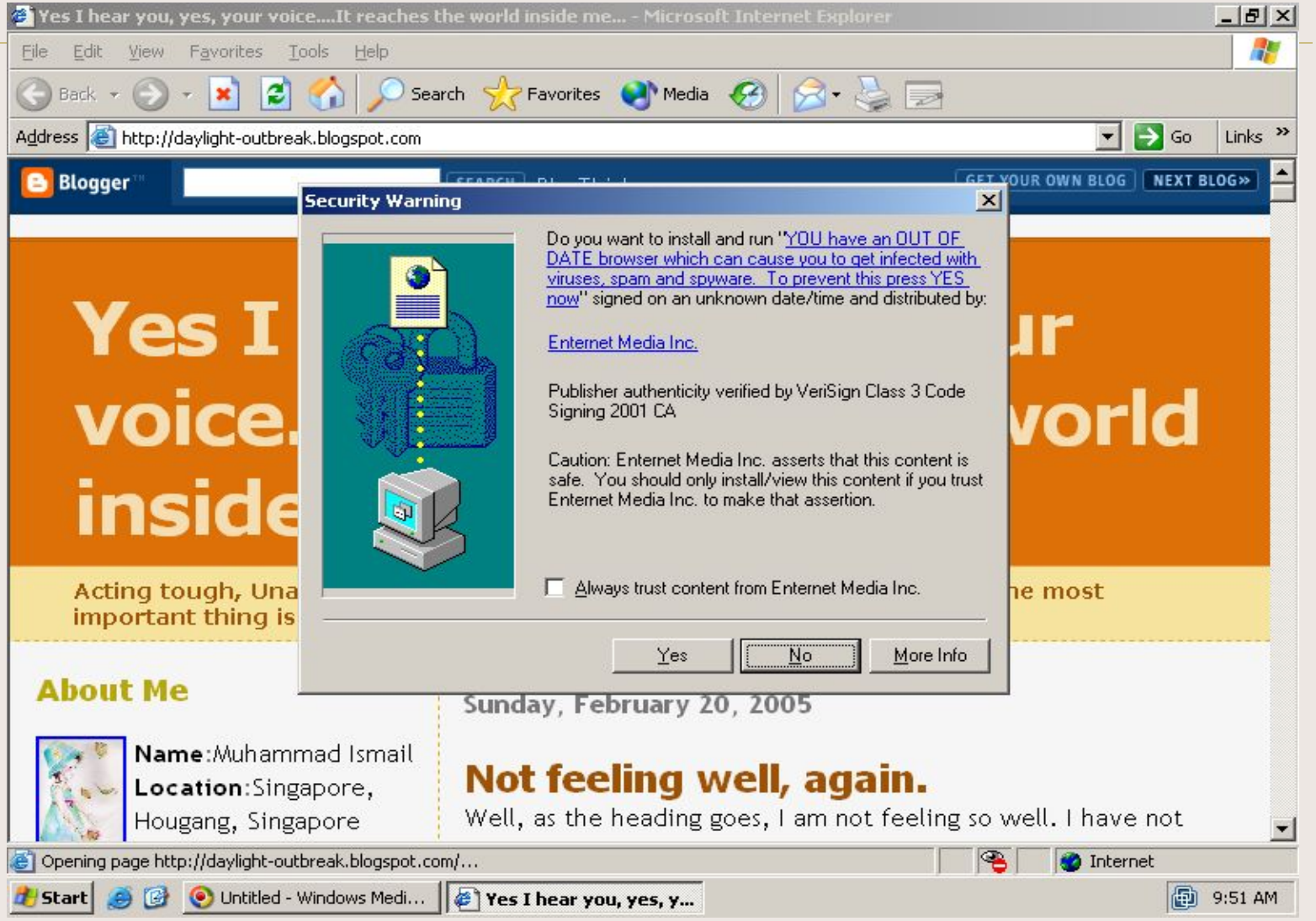
- A broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user
- In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet

Definitions

Spyware:

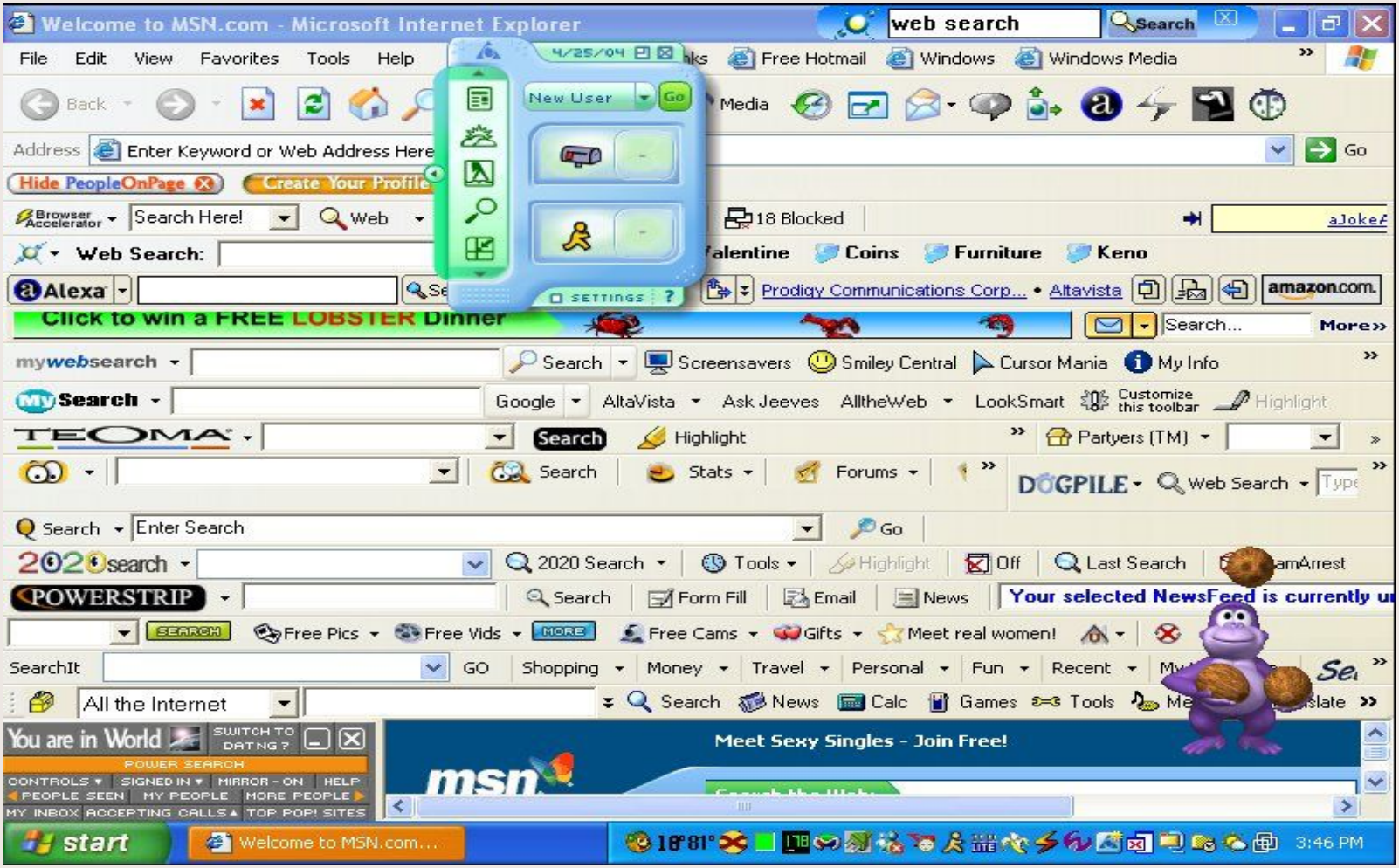
- Spyware can collect many different types of information about a user:
  - Records the types of websites a user visits
  - Records what is typed by the user to intercept passwords or credit card numbers
  - Used to launch “pop up” advertisements
- Many legitimate companies incorporate forms of spyware into their software for purposes of advertisement(Adware)

Spyware Example



Spyware Example

(add-on toolbars)

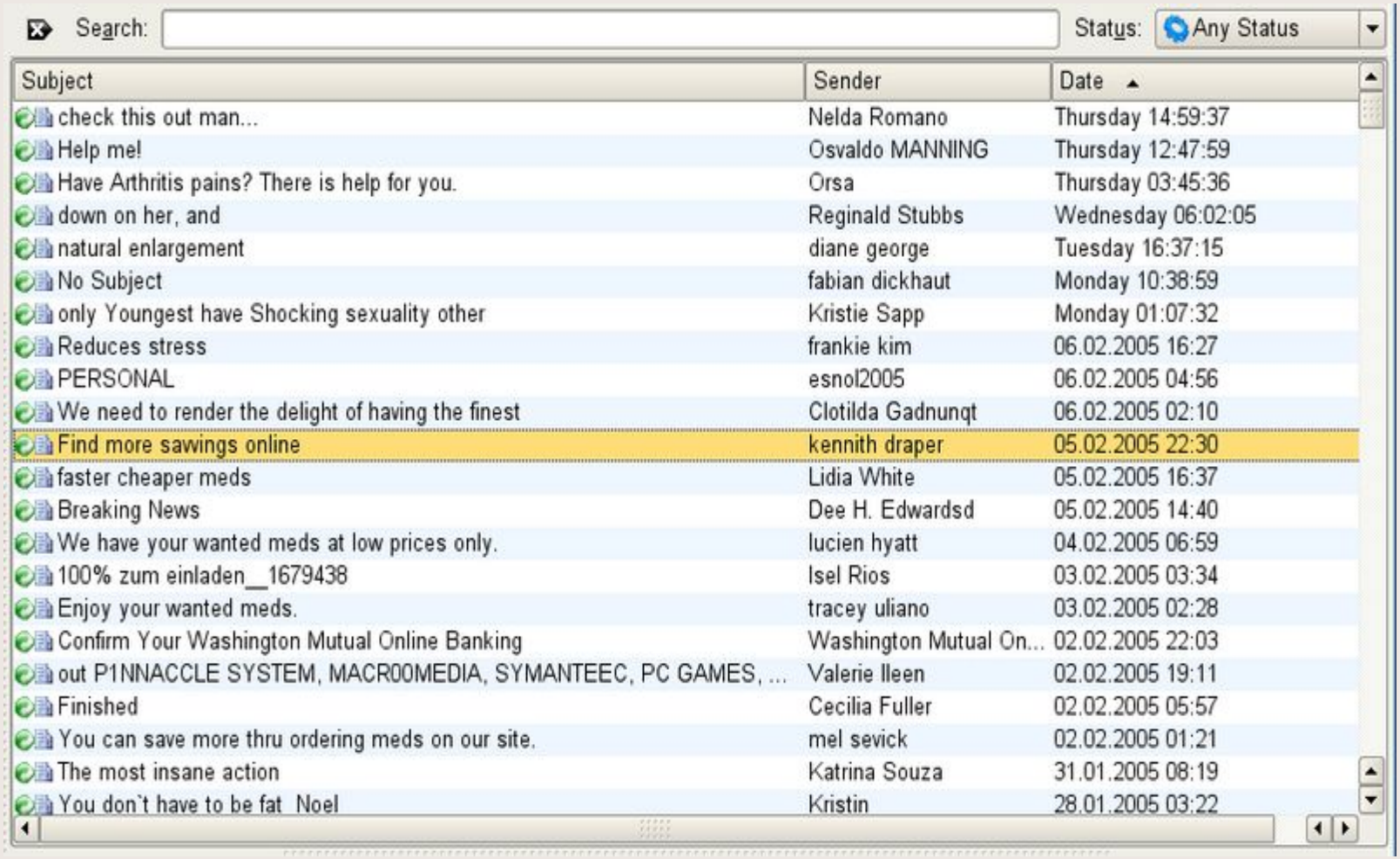


Definitions

Spam:

- **Spamming** is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages
- Spam media includes:
  - e-mail spam (most widely recognized form)
  - instant messaging spam
  - Usenet newsgroup spam
  - Web search engine spam
  - spam in blogs
  - mobile phone messaging spam

Spam Example



Definitions

Phishing:

- A criminal activity using social engineering techniques.
- An attempt to acquire sensitive data, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.
- Typically carried out using emailTypically carried out using email or an instant message

Phishing Example

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Points to "bad" IP Address!

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Definitions

Keystroke Logging:

- Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes
  - Useful to determine sources of error in computer programs
  - Used to measure employee productivity on certain clerical tasks
- Highly useful for law enforcement and espionage
  - Obtain passwords or encryption keys and thus bypassing other security measures
- Widely available on the internet and can be used by anyone for the same purposes

Definitions

Keystroke Logging:

- Can be achieved by both hardware and software means
- Hardware key loggers are commercially available devices which come in three types:
  - Inline devices that are attached to the keyboard cable
  - Devices installed inside standard keyboards
  - Keyboards that contain the key logger already built-in
- Writing software applications for keylogging is trivial, and like any computer program can be distributed as malware (virus, trojan, etc.)

Keylogger Example

In-line hardware Keylogger

Viruses, Bots, and Phish, Oh My!

Why is it Important?

- Over the last two years, the IT security threat landscape has changed significantly.
- Traditional malware threats hit an apparent wall in 2005
- However new threats (bots, spam, phishing) have stepped into the void.
- Remember the objective - the “CIA Triad” :
  - Confidentiality
  - Integrity
  - Availability (Recoverability)

Viruses, Bots, and Phish, Oh My!

Why is it Important?

- Unauthorized access (malware, spyware) limits our ability to protect the confidentiality of the data
- Malicious programs can alter the data values, destroying the integrity of the data
- Denial of Service (DoS) attacks can shut down a server and/or network, making the system unavailable.
- Efforts to correct costs corporations time and money!

Viruses, Bots, and Phish, Oh My!

Why is it Important?

- There were on average over eight million phishing attempts per day during the latter half of 2005 (Symantec)
- The California legislature found that spam cost United States organizations alone more than $10 billion in 2004, including lost productivity and the additional equipment, software, and manpower needed to combat the problem.

Viruses, Bots, and Phish, Oh My!

Why is it Important?

- Regulatory Issues:
  - HIPAA (electronic personal identifiable information)
  - Sarbanes-Oxley Act (federal securities law focused on data accuracy and integrity)
  - PCI Security (Payment Card Industry security measures)
- Potential/Growing Issues:
  - Liability for damage caused by bot-nets
  - Loss of corporate confidential information (financials, personnel)
  - Electronic Blackmail

Viruses, Bots, and Phish, Oh My!

What Can We Do?

- Security Assessment
  - Identify areas of risk
  - Identify potential for security breaches, collapses
  - Identify steps to mitigate
- Security Application
  - Expert knowledge (train, hire, other)
  - Multi-layered Approach (there is no single solution)
  - Policies and Procedures

Viruses, Bots, and Phish, Oh My!

What Can We Do?

- Security Awareness
  - Not just for the geeks!
  - Security Training at all levels (external and/or internal)
  - Continuing education and awareness – not a one-time shot!
  - Make it part of the culture

Viruses, Bots, and Phish, Oh My!

Key Takeaways:

- Objective of InfoSec is ***Confidentiality, Integrity and Availability***…protect your systems and your data
- Threats are numerous, evolving, and their impact is costly
- Security should be applied in layers (“road blocks”)
- Security Awareness at all levels must be maintained
- Failure to Secure is an Opportunity to Fail

Information Security

Questions?