INTERNET SECURITY OVERVIEW

AfNOG

9th June 2013 – 14th June 2013

Lusaka, Zambia

By

Marcus K. G. Adomey

OUTLINE

- **INFORMATION SYSTEM SECURITY**
  - Brainstorm:- Internet and Security
  - Definition
  - Features
  - Types of Security
  - Incidents
  - Types of Security Incidents
  - Vulnerabilities
  - The Way forwards

BRAINSTORM

Internet and Security

Internet

"The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide."

"It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies."

Source: WIKIPEDIA

- *Everybody use it*

Ladies in the market

Shepherds use the it to locate cattle

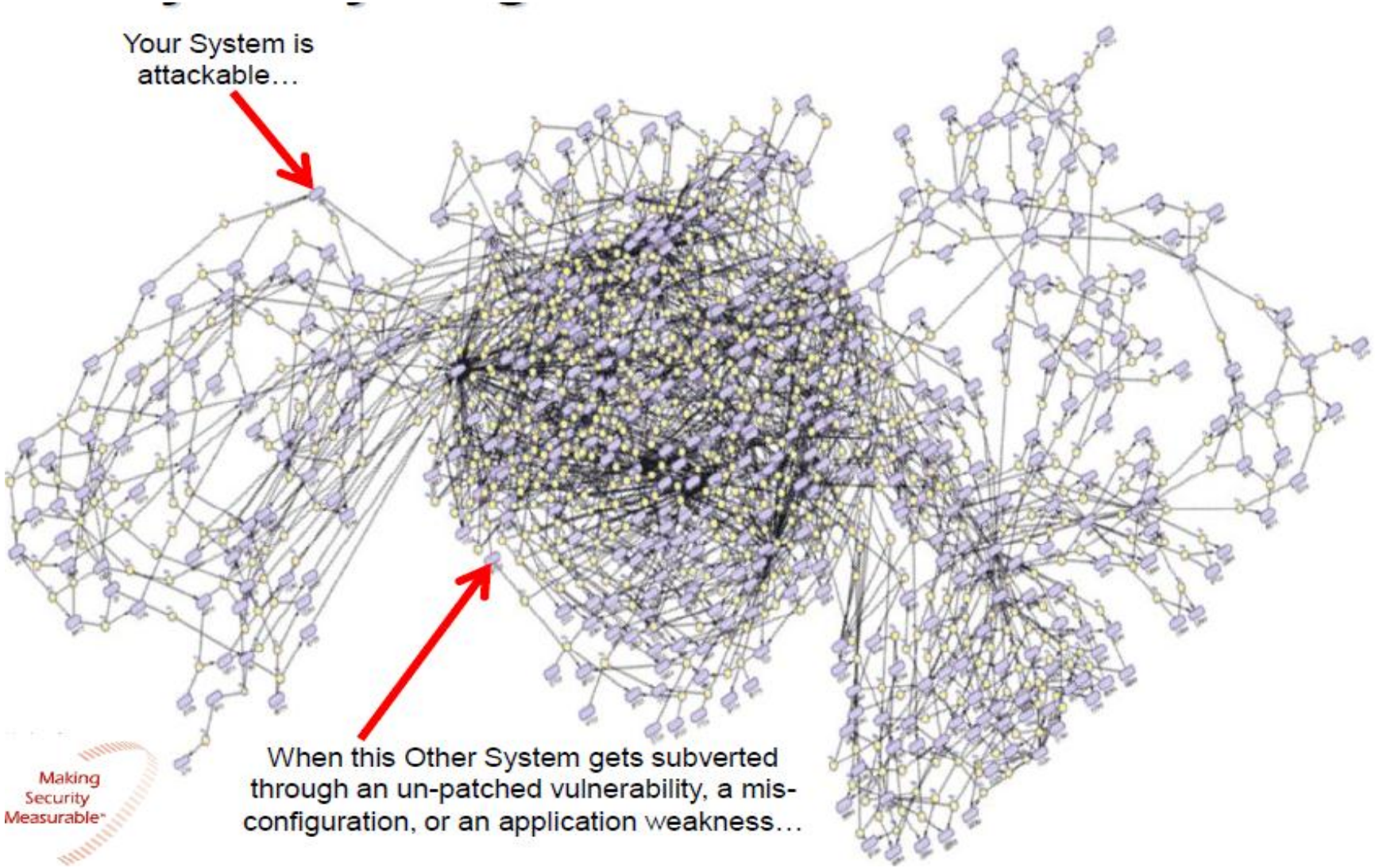
Hunters use it to locate their prey

Farmers use it even when they are in the tree

Huum! isn’t amazing? They are also using it.


VAIO

PROBLEMS


Your System is attackable…
When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…
Making Security Measurable™

BRAINSTORM

Movie:- Trojan Horse and Spyware

In this borderless space (cyberspace) insecurity is being modernised

We are faced with what is known as cybercrime which is refers to any crime that involves a computer and a network.

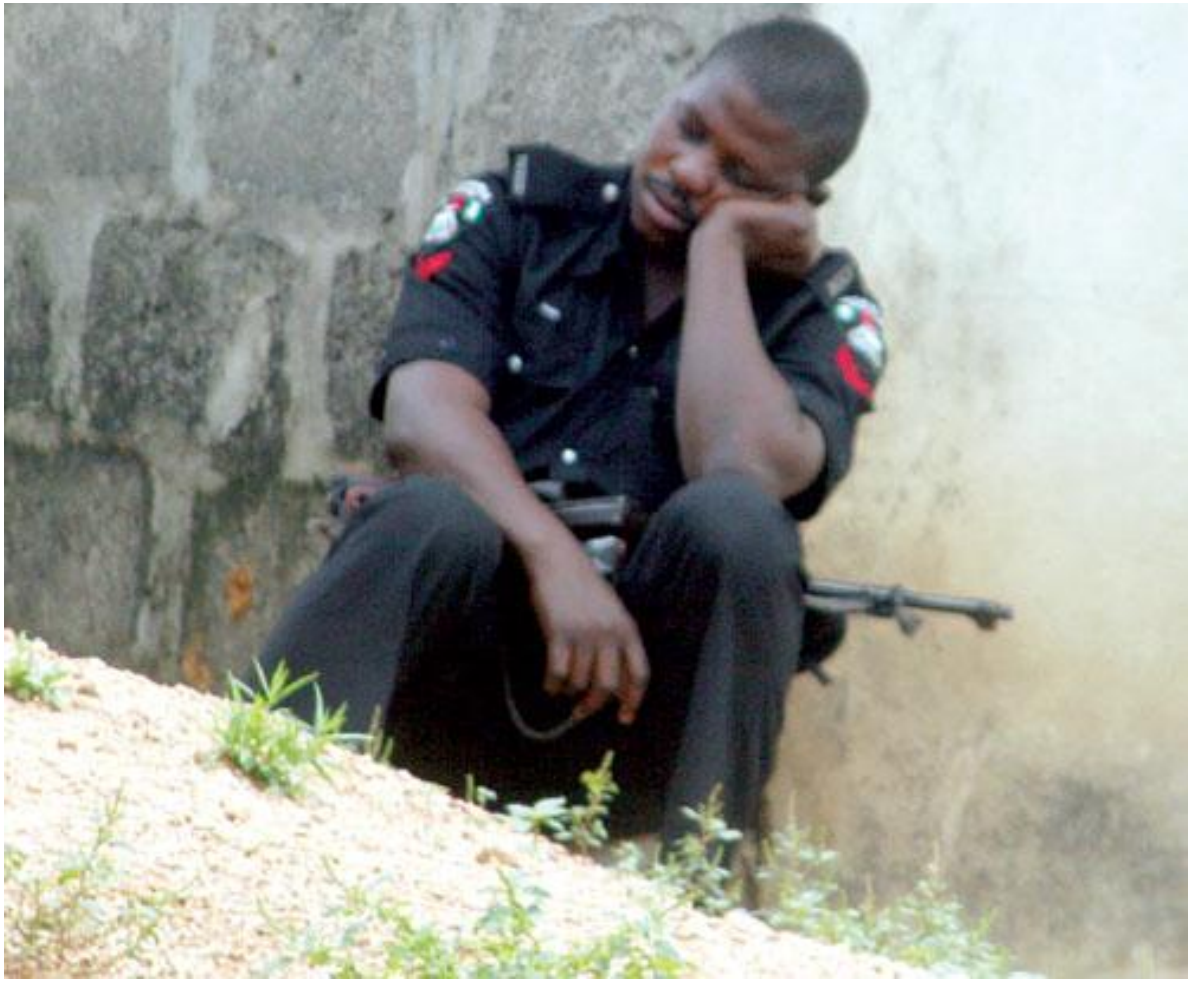
It is becoming more and more sophisticated

QUESTION

What is security?

BRAINSTORM

cont.



POLICE MAN

BRAINSTORM

cont.

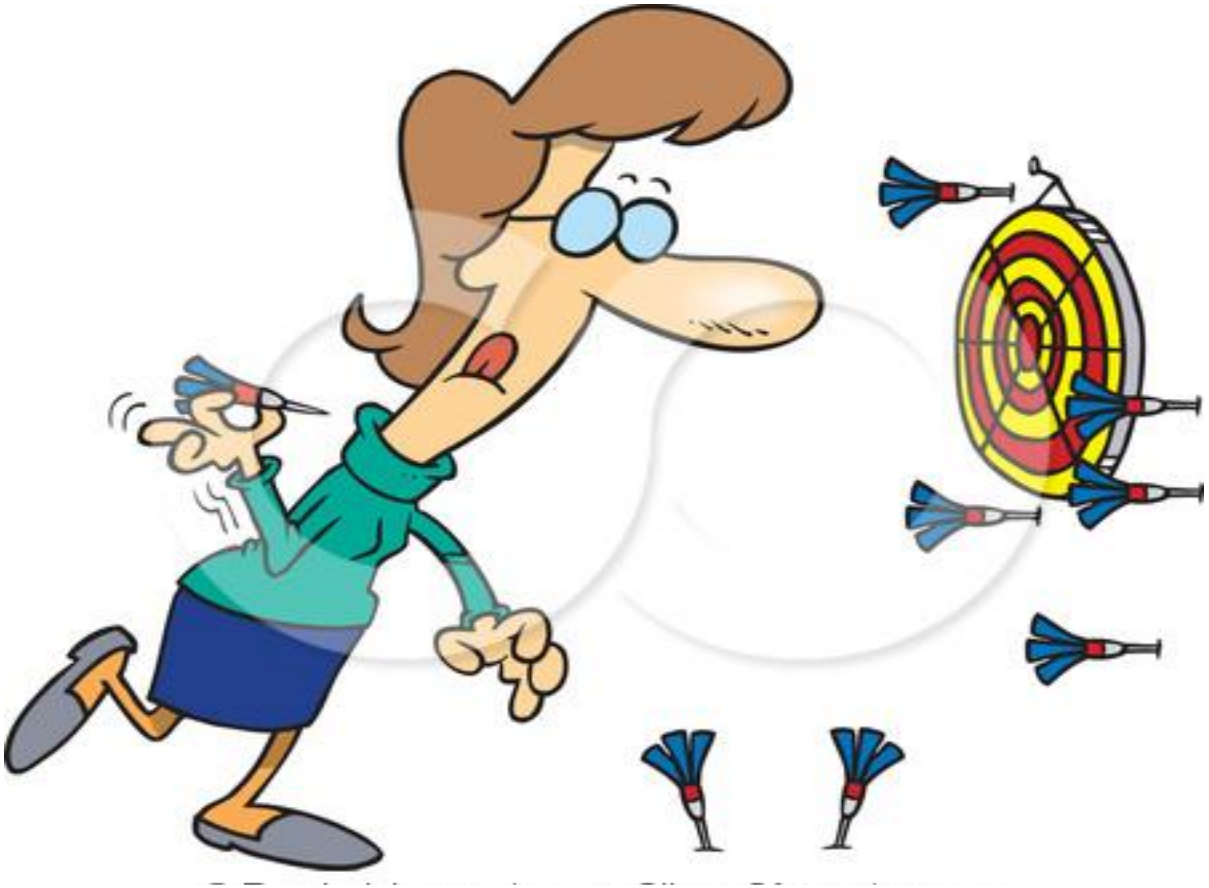
BRAINSTORM

What is Security?

DEFINITION

DEFINITION

FACT:- ***There is no clear cut definition***



DEFINITION

cont.

Security is a process, not an end state.

DEFINITION

No organization can be considered **"secure"** for any time beyond the last verification of adherence to its security policy.

- **If your manager asks** ***"Are we secure?"***
- **You should answer**, ***"Let me check."***
- **If he or she asks**, ***"Will we be secure tomorrow?"***
- **You should answer**, ***"I don't know."***

Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

QUESTIONS

FEATURES

FEATURES

The key aspect of Information Security is to preserve the confidentiality, integrity and availability **(CIA)** of an organization's information.

- **Confidentiality.** Assurance that information is shared only among authorized persons or organizations.
- **Integrity.** Assurance that the information is authentic and complete.
- **Availability**. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

TYPES OF SECURITY

TYPES OF SECURITY

Access Control

- Categories and Controls
- Control Threats and countermeasures

Application Development Security

- Software Based Controls
- Software Development Lifecycle and Principles

Business Continuity and Disaster Recovery Planning

- Response and Recovery Plans
- Restoration Activities

Cryptography

- Basic Concepts and Algorithms
- Signatures and Certification
- Cryptanalysis

TYPES OF SECURITY cont.

Information Security Governance and Risk Management

- Policies, Standards, Guidelines and Procedures
- Risk Management Tools and Practices
- Planning and Organization,

Legal, Regulations, Investigations and Compliance

- Major Legal Systems
- Common and Civil Law
- Regulations, Laws and Information Security

Operations Security

- Media, Backups and Change Control Management
- Controls Categories

TYPES OF SECURITY

end

Physical (Environmental) Security

- Layered Physical Defense and Entry Points
- Site Location Principles

Security Architecture and Design

- Principles and Benefits
- Trusted Systems and Computing Base
- System and Enterprise Architecture

Telecommunications and Network Security

- Network Security Concepts and Risks
- Business Goals and Network Security

An many more

SECURITY INCIDENTS

SECURITY INCIDENTS

Computer security incident activity can be defined as network or host activity that potentially threatens the security of computer systems.

SECURITY INCIDENTS

Examples of incidents could include activity such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

QUESTIONS

THREAT

An event, the occurrence of which could have an undesirable impact on the well-being of an asset.

[ISC2]
International Information Systems Security Certification Consortium

Any circumstances or event that has the potential to cause harm to a system or network .That means, that even the existence of a(n unknown) vulnerability implies a threat by definition.

[CERT]

TYPES OF SECURITY THREATS

- Malicious Code
- Denial of Service
- Unauthorized Access
- Inappropriate Usage

MALICIOUS CODE - MALWARE

Malware, short for MALicious softWARE, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or code.

Types of Malware

- ✓ Virus
- ✓ AdWare
- ✓ Spyware
- ✓ BotNet
- ✓ Worm
- ✓ Key Loggers
- ✓ Rootkits

Virus

A virus program contains instructions to initiate some sort of "event" that affects the infected computer. Each virus has a unique event associated with it. These events and their effects can range from harmless to devastating. For examples:

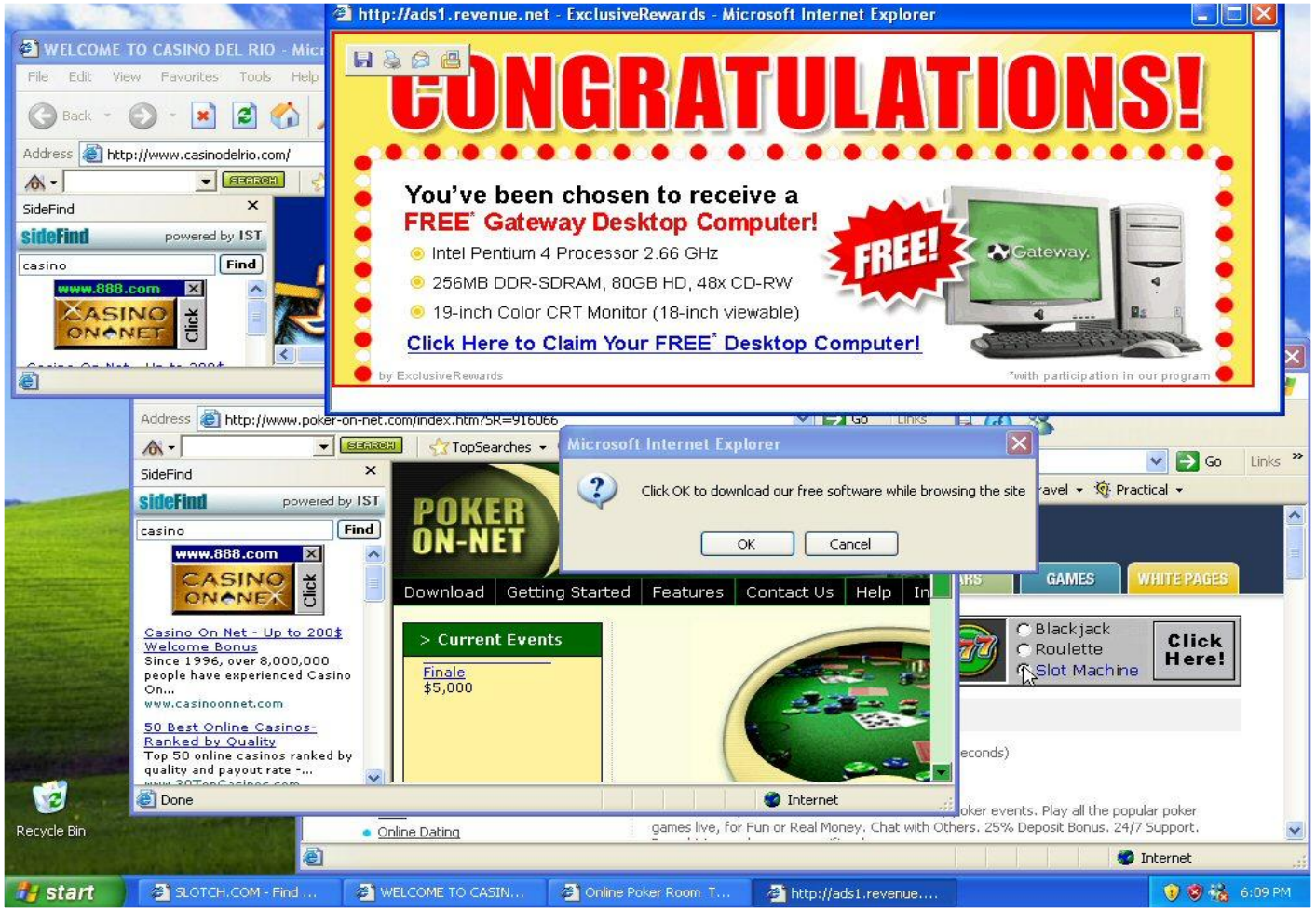
- ✓ An annoying message appearing on the computer screen.
- ✓ Reduced memory or disk space.
- ✓ Modification of data.
- ✓ Files overwritten or damaged.
- ✓ Hard drive erased.

AdWare (ADvertising-supported softWARE)

A software program that is designed to run once a web page has been accessed. This is usually in the form of banner or popup advertisements.

- ✓ Adware are designed to be installed on systems without the user consent or knowledge.
- ✓ Some adware track the Internet surfing habits of the users in order to serve ads related to them. When the adware becomes intrusive like this, it is then considered as a spyware

AdWare (ADvertising-supported softWARE)



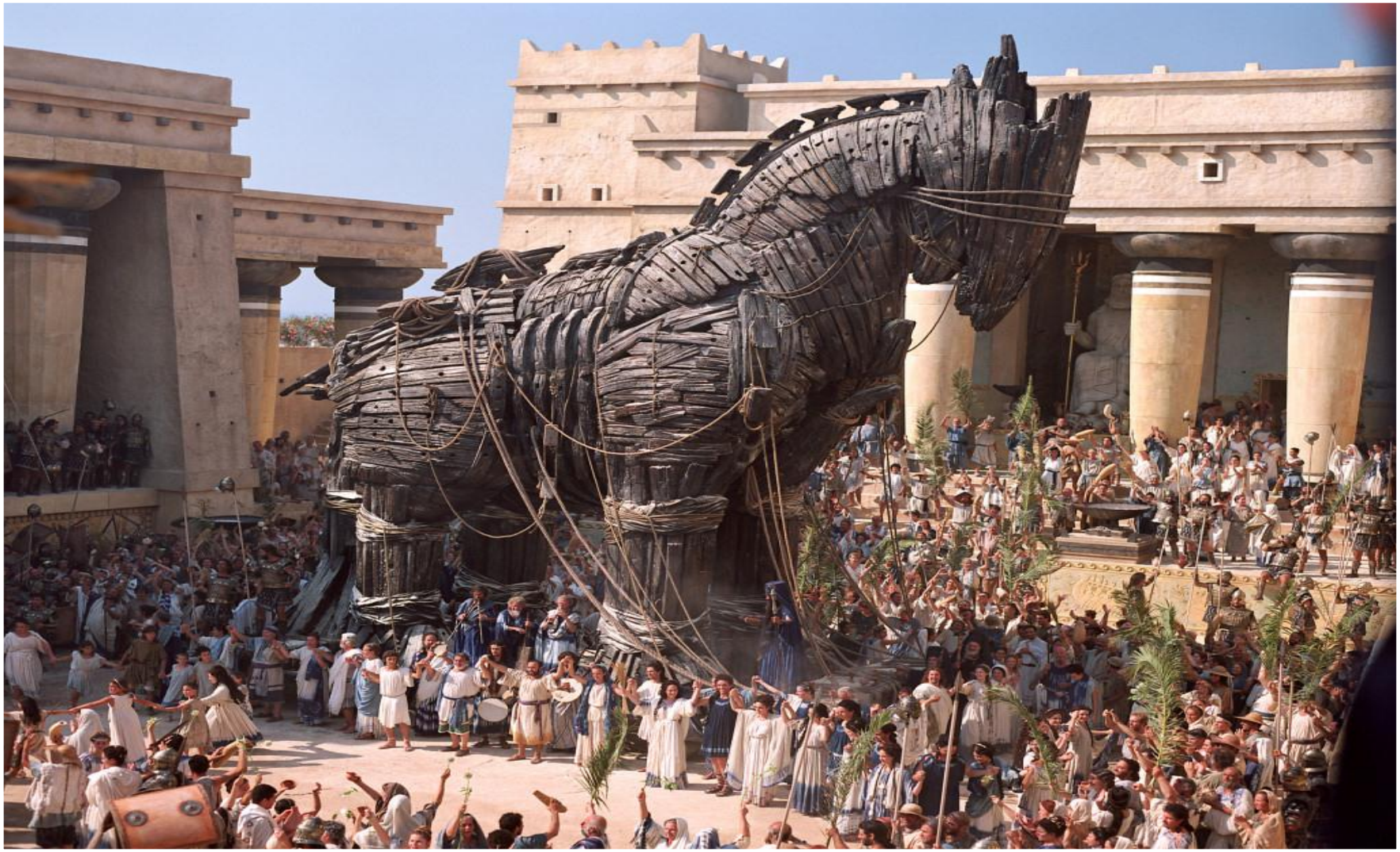
Adware displayed on the PC

Spyware

Spyware is a type of program that can be installed on computers and is designed to steal confidential information (eg. credit card details, user names, passwords etc.) of the PCs users without their knowledge.

- ✓ The presence of spyware is typically hidden from the user, and can be difficult to detect.
- ✓ Software downloaded from the Internet may contain spyware and other forms of malware.

Trojan horse



Trojan horse

- ✓ The name comes from the mythical “Trojan Horse” that the Ancient Greeks set upon the city of Troy.
- ✓ A trojan horse secretly carries damaging software in the guise of an innocuous program, often as an email attachment.
- ✓ If opened, it will scour your hard drive for any personal and financial information such as your social security, account, and PIN numbers. Once it has collected your info, it is sent to a thief’s database.

BotNet

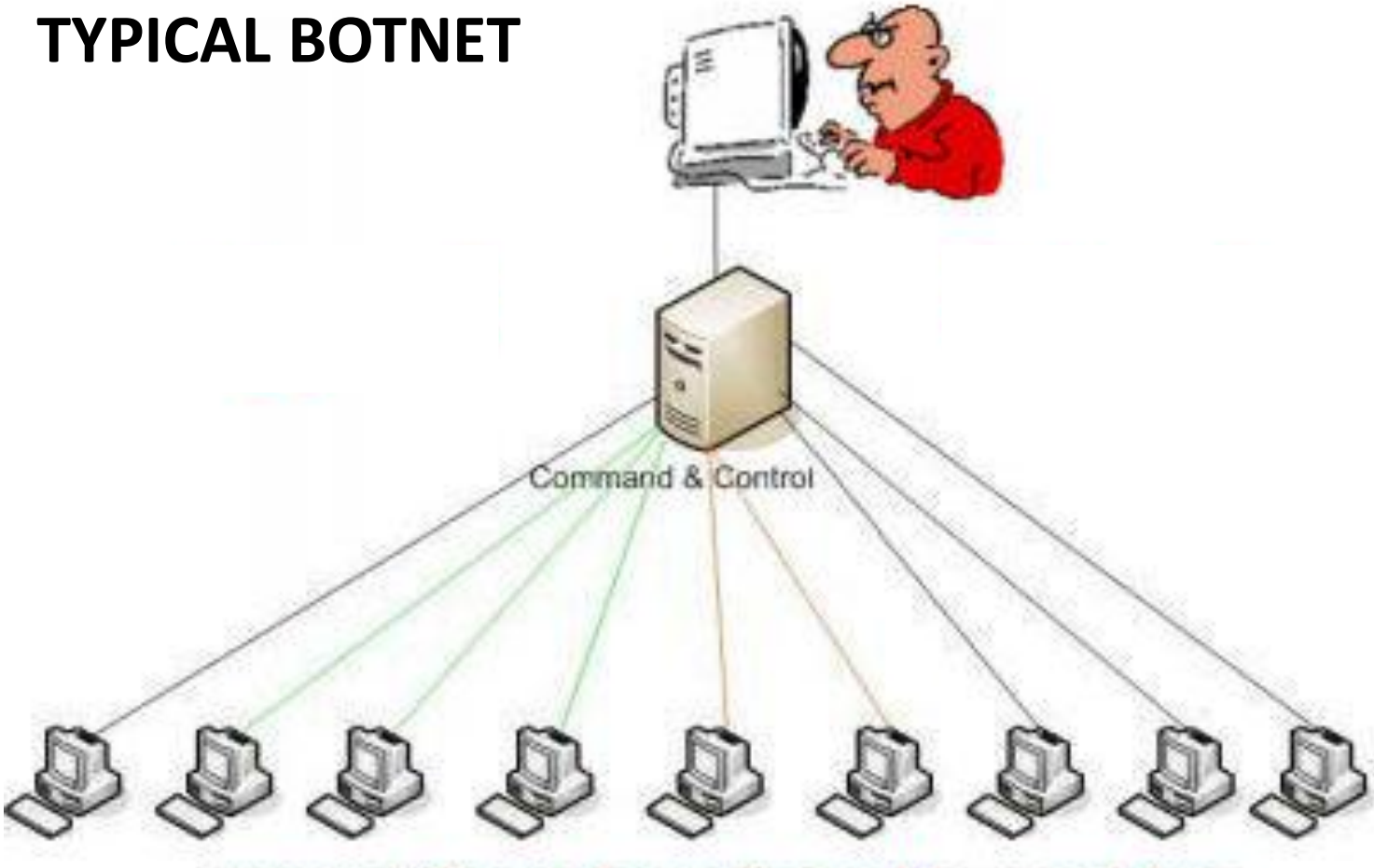
A botnet or ro**BOT NET**work is a group of compromised computers running a computer application controlled and manipulated only by the owner or the software source.

- ✓ The compromised computer ("robot", "bot", zombie or a drone) participating in such network runs a piece of programme is controlled by a Bot Herder or Bot Master who give them commands.

- ✓ The computer is compromised via a Trojan.

BotNet

TYPICAL BOTNET



ZOMBIES

Uses of BotNets

Botnets are used for both recognition and financial gain.

- The larger the botnet, the more ‘kudos’ the bot herder' could claim in underground, online communities.

- A botnet can have a lot of malicious applications. Among the most popular uses of botnets are the following:
  - ✓ Denial of Service Attacks
  - ✓ Spamming and Traffic Monitoring
  - ✓ Keylogging and Mass Identity Theft
  - ✓ Botnet Spread
  - ✓ Pay-Per-Click Systems Abuse

Uses of BotNets

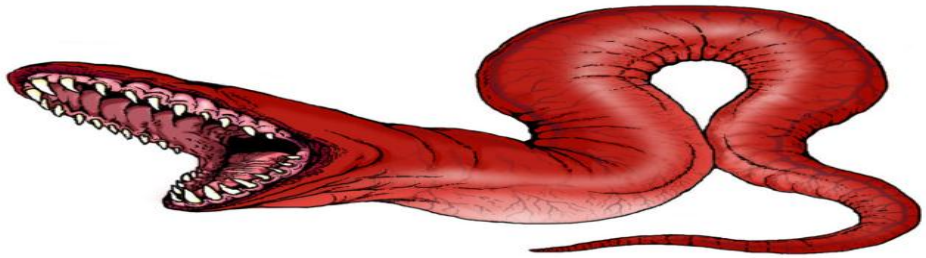
- ✓ A bot herder can ‘rent out’ the services of the botnet to third parties to perform the above uses.
- ✓ A bot can be sold out
- ✓ A bot can be stolen

MOVIE - BotNet

Computer worms

A computer worm is a self-replicating computer programme that has the ability to send copies of itself to other computers on the network.

A worm usually exploits some sort of security hole in a piece of software or the operating system.



Example of Worms

Morris worm

- ✓ Morris worm was the first and fast self-replicating computer worms distributed via the Internet
- ✓ Crippled almost 10 percent (6000) of the computer connected to the Internet in Nov 1988.

Stuxnet

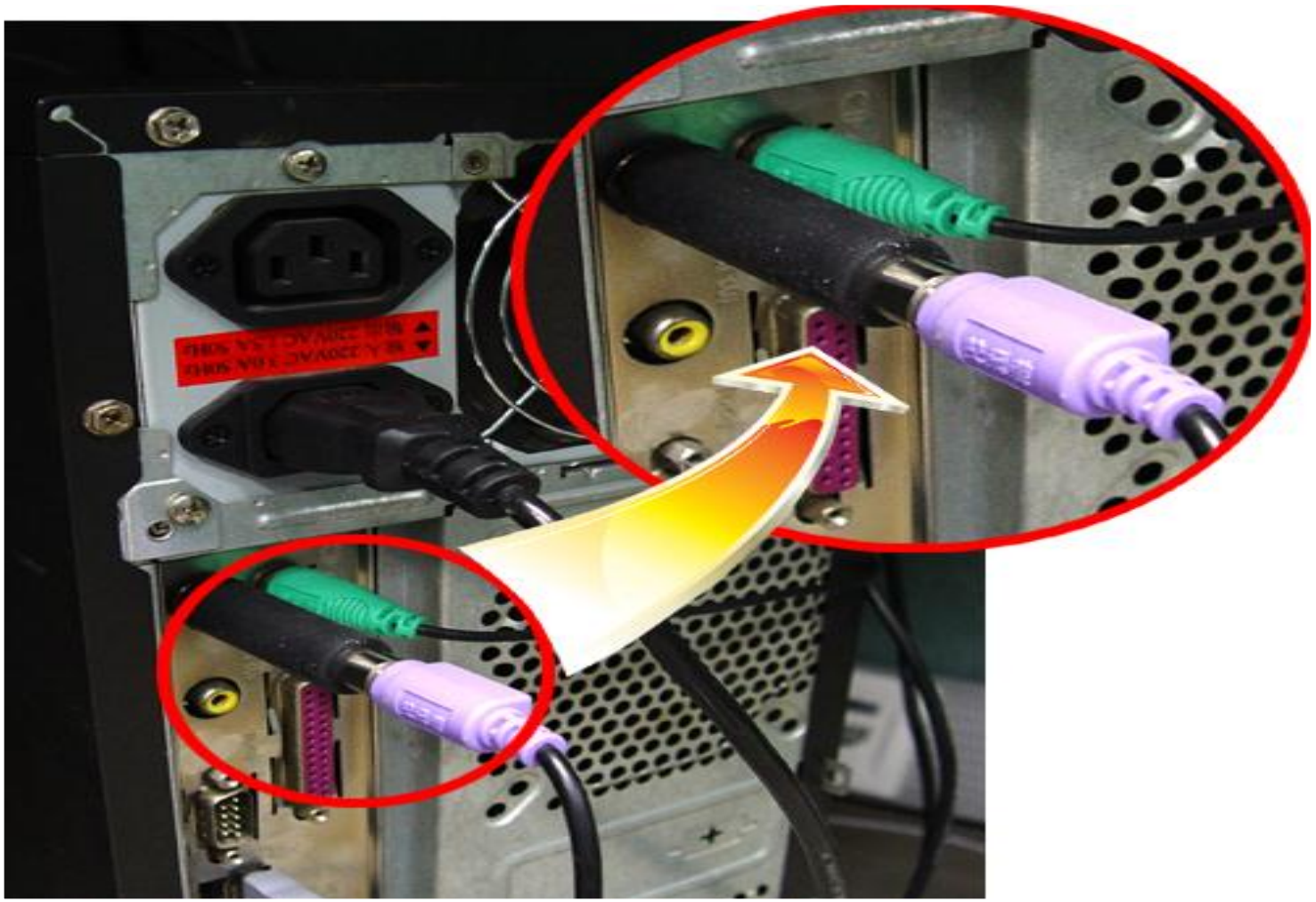
- ✓ A highly sophisticated computer worm that has spread through Iran, Indonesia and India was built to destroy operations at one target: possibly Iran's Bushehr nuclear reactor.

Key loggers

A key logger is a tool designed to record every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data.

Key loggers

Key loggers



Rootkit

It is designed to conceal the existence of certain malware on the compromise computer system and works to subvert control of an operating system from its legitimate operators. It allows the attacker to mask intrusion and gain root or privileged access to the computer and among others

- create a "backdoor" into the system for the hacker's use;
- monitors traffic and keystrokes;
- alter log files;
- and attack other machines on the network;

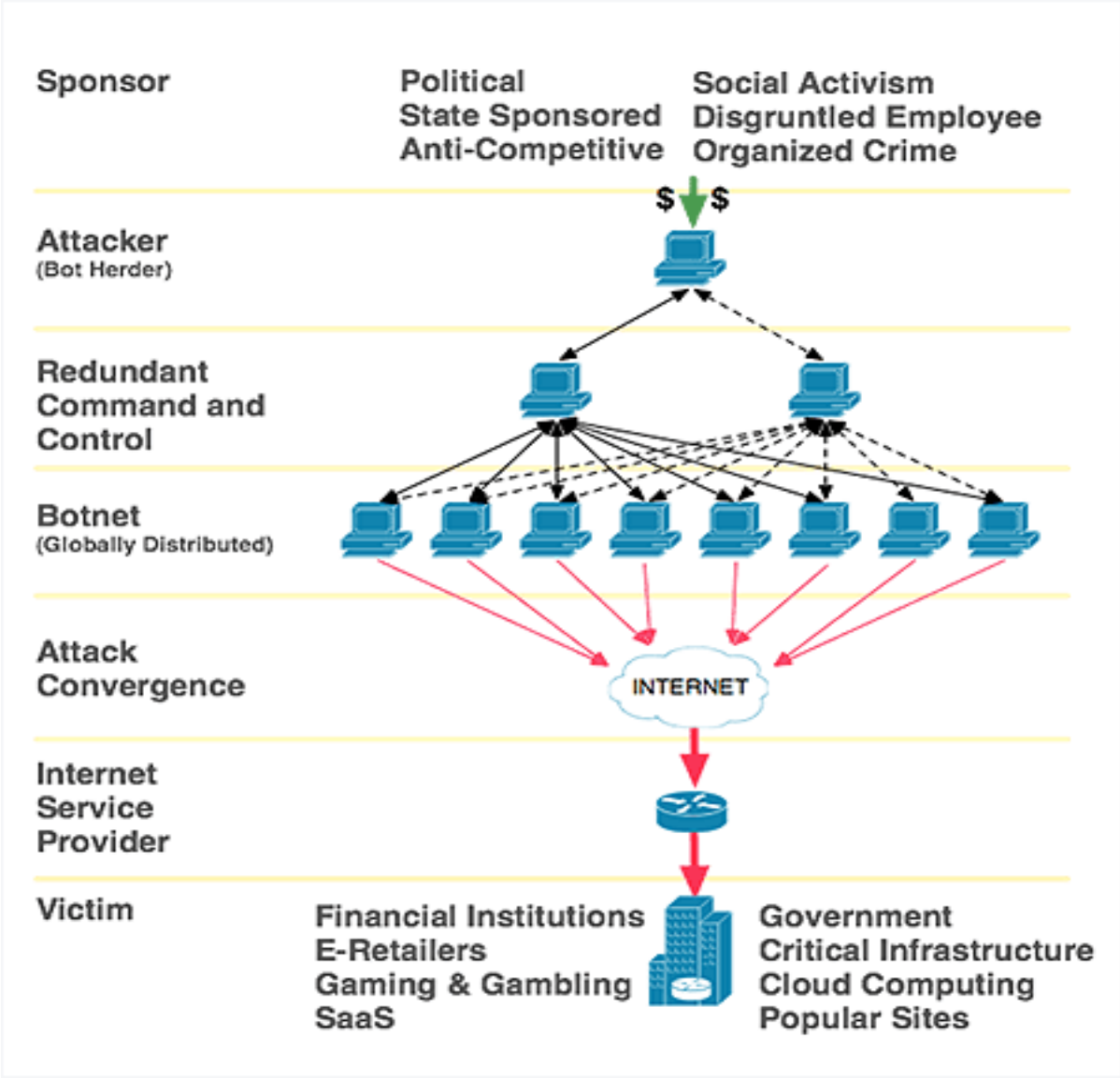
QUESTIONS

DENIAL OF SERVICE

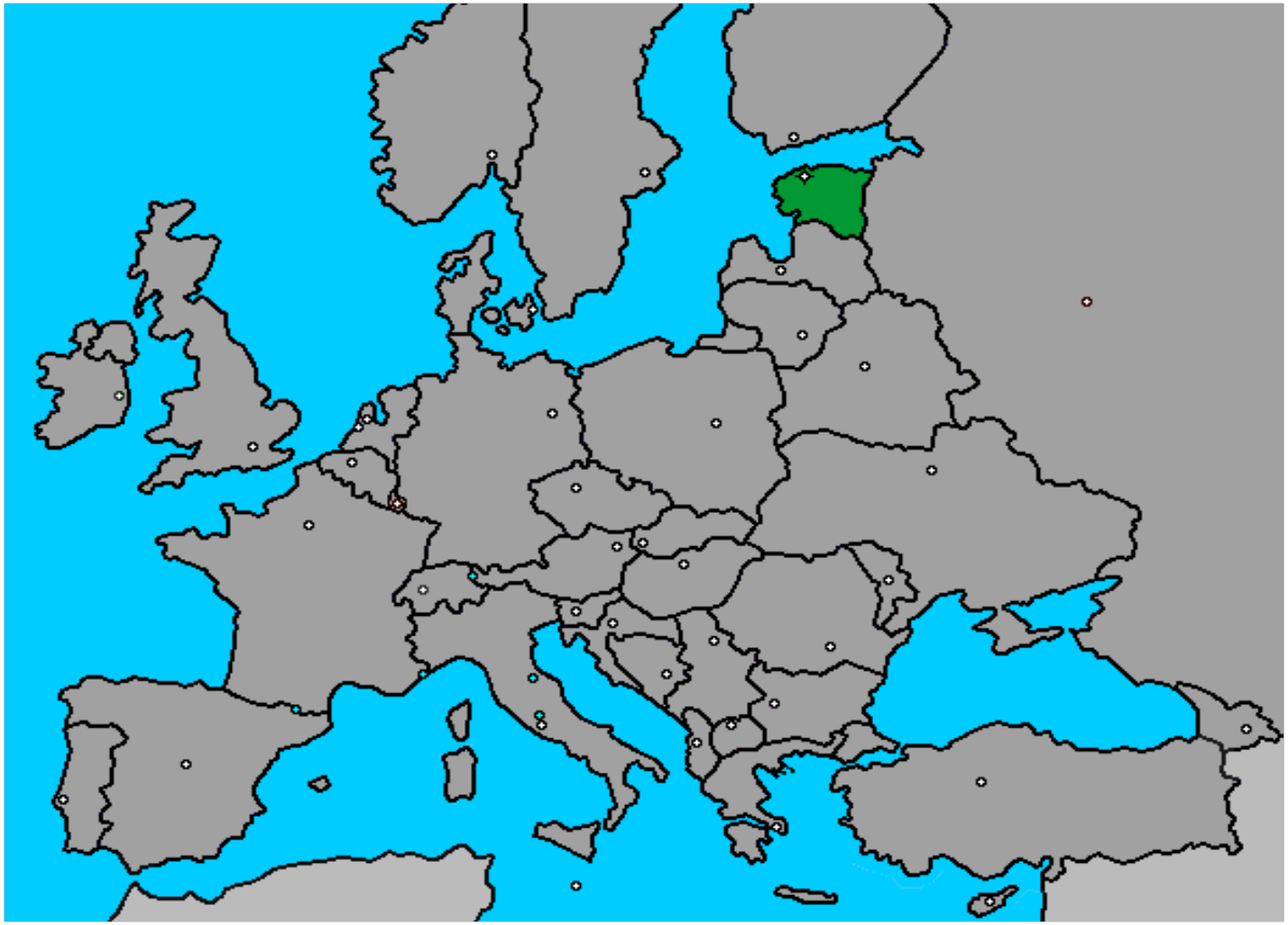
A denial-of-service (DoS) attack or Distributed Denial-Of-Service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

- or -

A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space.


Sponsor
Political
State Sponsored
Anti-Competitive
Social Activism
Disgruntled Employee
Organized Crime
$ $
Attacker
(Bot Herder)
Redundant
Command and
Control
Botnet
(Globally Distributed)
Attack
Convergence
INTERNET
Internet
Service
Provider
Victim
Financial Institutions
E-Retailers
Gaming & Gambling
SaaS
Government
Critical Infrastructure
Cloud Computing
Popular Sites

Estonia Cyber Attacks Case



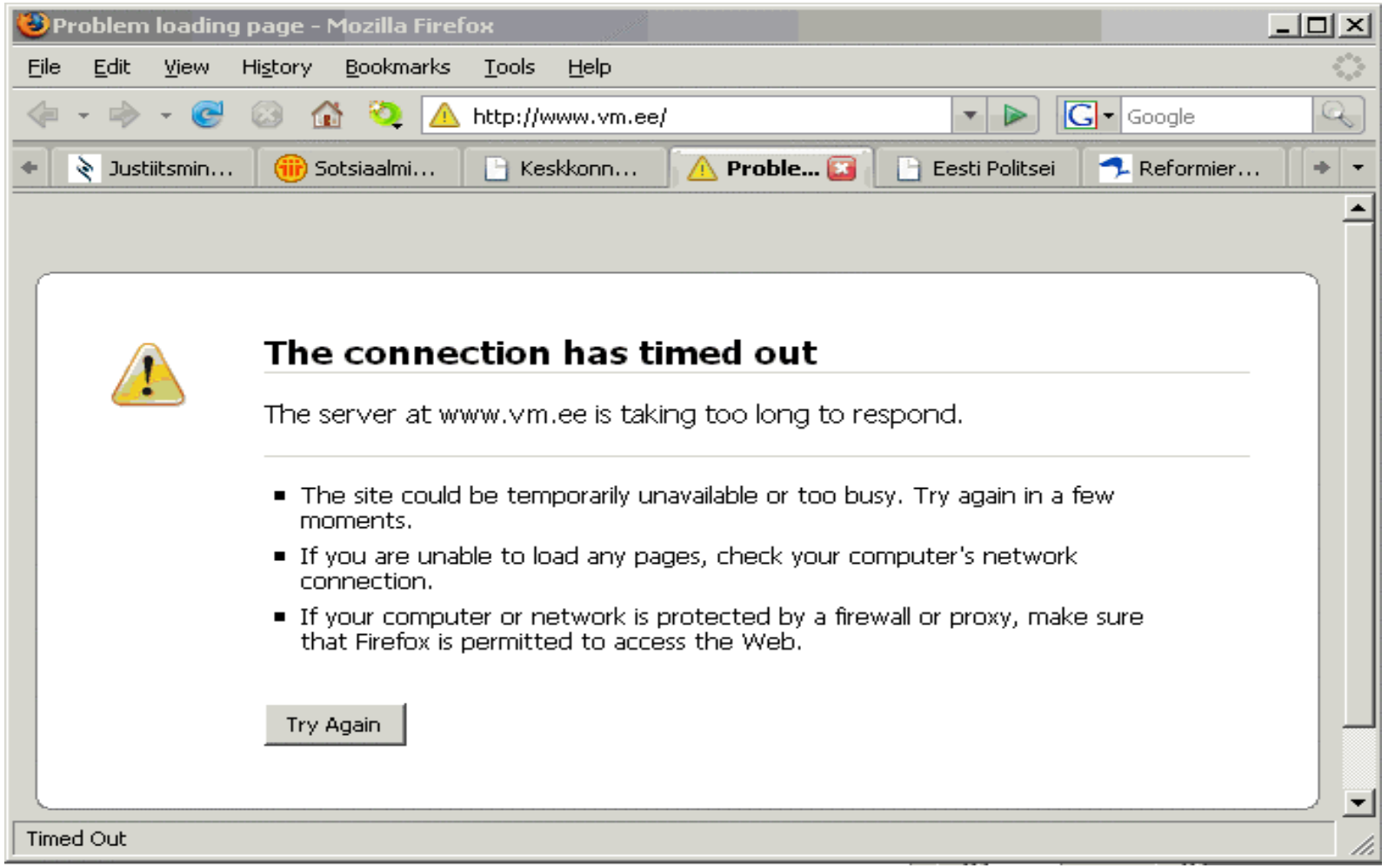
Why Estonia Cyber Attacks?

The Bronze Soldier Alyosha, located in the centre of Tallinn, erected during the Soviet regime.

- ✓ For many Russians (in Estonia) the monument was one of the few remaining symbols that connected them to Russia and Russian identity.
- ✓ For Estonian nationalists this monument was the symbol for Soviet occupation and marked the beginning of Stalinist repressions.
- ✓ On 27 April 2007, the Estonian government moved a controversial Soviet-era World War II memorial from a square in the capital city of Tallinn to a cemetery.

AFNOG

- ✓ Protests erupted in Estonia and Russia, where Estonia's Moscow embassy was blockaded.
- ✓ The Russian government protested vociferously and issued threats.
- ✓ Weeks of cyber attacks followed, targeting government and banks, ministries, newspapers and broadcasters Web sites of Estonia.
- ✓ Access to the banks, government agencies website become unavailable such as Estonian national Web sites, including those of government ministries and the prime minister's Reform Party.
- ✓ A flood of junk messages was thrown at the e-mail server of the Parliament, shutting it down.


Problem loading page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.vm.ee/
Google
Justiitsmin...
Sotsiaalmi...
Keskkonn...
Proble...
Eesti Politsei
Reformier...
The connection has timed out
The server at www.vm.ee is taking too long to respond.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again
Timed Out

Tuuli Aug, an editor of the daily newspaper "Eesti Paevaleht," stated the following:

"I felt the country was under attack by an invisible enemy. . . . It was extremely frightening and uncontrollable because we are used to having Internet all the time and then suddenly it wasn't around anymore, . . . You couldn't get information; you couldn't do your job. You couldn't reach the bank; you couldn't check the bus schedule anymore. It was just confusing and frightening, but we didn't realize it was a war because nobody had seen anything like that before".

UNAUTHORIZED ACCESS

Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner.

The popular term for this is "hacking".

Type of Hackers

- White hat - perform penetration tests and vulnerability assessments within a contractual agreement.

- Black Hat - break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.
- Grey hat - hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.
- Neophyte - someone who is new to hacking
- Script kiddie - non-expert who breaks into computer systems by using pre-packaged automated tools written by others.

Types of Hacking

External Hacking

Attacks where the intruder has no privilege on the target network, and either gains access from outside the network perimeter or by evading or undermining the target's physical and/or network security measures to achieve some degree of access to the target's internal network.

Internal Hacking

Attacks where the intruder has legitimate privileges on the target network. Access is obtained using existing privileges, privileges the intruder has extended without permission, or privileges stolen from other users.

Commonwealth Bank ATM Case, Australia

Commonwealth Bank, Australia - March 2011:- Automatic teller machines (ATMs) spat out tens of thousands of free dollars in Sydney Tuesday after a computer glitch turned into a nightmare for the Commonwealth Bank. IT Security Believe that it is a the consequence of hacking.

INAPPROPRIATE USAGE

An inappropriate usage incident occurs when a user performs actions that violate acceptable computing use policies.

Examples:

- Download password cracking tools or pornography
- Send spam promoting a personal business
- E-mail harassing messages to coworkers
- Set up an unauthorized Web site on one of the organization's computers
- Use file or music sharing services to acquire or distribute pirated materials
- Transfer sensitive materials from the organization to external locations.
- Violating terms of applicable software licensing agreements or copyright laws
- Failing to adhere to individual departmental or unit lab system policies, procedures, and protocol

Social Engineering

There exist several definitions

- ✓ “the art and science of getting people to comply to your wishes”
- ✓ “an outside hacker’s use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system”
- ✓ “getting needed information (for example, a password) from a person rather than breaking into a system”

Social Engineering

The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust.

The basic goal of social engineering is to obtain information that will allow the hacker to gain unauthorized access to a valued system and the information that resides on that system.

Social Engineering

Types of social engineering

- Social Engineering at workplace
- Shoulder Surfing
- Social Engineering by phone
- Dumpster Diving (also known as trashing)
- Online Social Engineering
- Reverse Social Engineering

Social engineering

Social Engineering at workplace

In the workplace, the hacker can simply walk in the door, like in the movies, and pretend to be a maintenance worker or consultant who has access to the organization. Then the intruder struts through the office until he or she finds a few passwords lying around and emerges from the building with ample information to exploit the network from home later that night.

Social Engineering

Movie: Social Engineering at workplace

Shoulder Surfing

Another technique to gain authentication information is to just stand there and watch an oblivious employee type in his password. This is also known as **Shoulder Surfing**

Social Engineering by phone

Intimidation:- the hacker attacks the person who answers the phone with threats to their job. Many people at this point will accept that the hacker is a supervisor and give them the needed information

Helpfulness :- the hacker takes advantage of a person natural instinct to help someone with a problem. The hacker will not get angry instead act very distressed and concerned. The help desk is the most vulnerable to this type of attack, because they generally have the authority to change or reset passwords which is exactly what the hacker needs

Name-Dropping :- Simply put the hacker uses the names of advanced users as "key words", and gets the person who answers the phone to believe that they are part of the company because of this. Some information, like web page ownership, can be obtained easily on the web. Other information such as president and vice president names might have to be obtained via dumpster diving.

Dumpster Diving (also known as trashing)

- A huge amount of information can be collected through company dumpsters.
- The following items as potential security leaks in our trash: "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware."

Reverse Social Engineering

This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around.

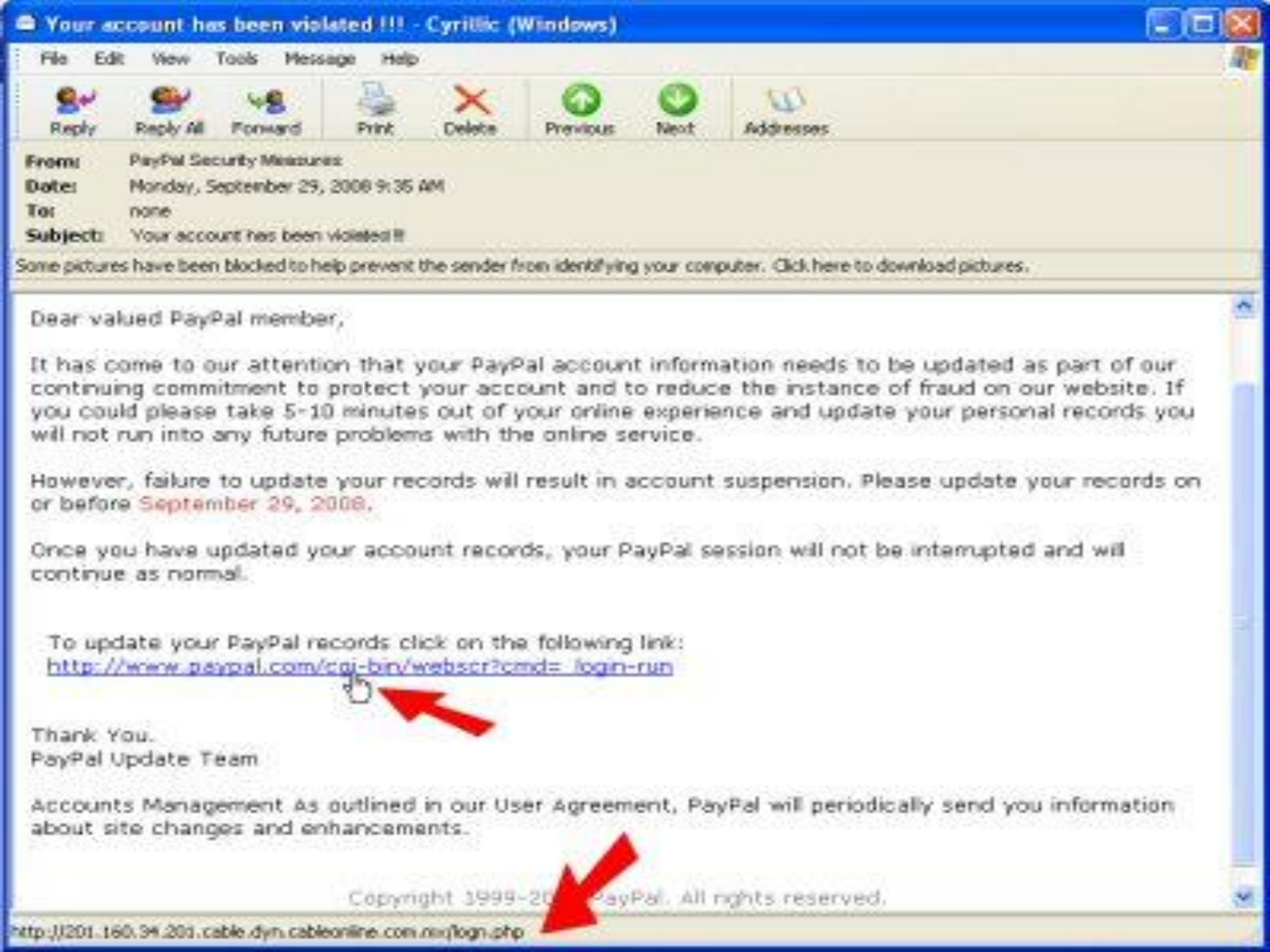
If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees; however, this requires a deal of preparation, research, and pre-hacking to pull off.

Online Social Engineering

Technical Using technology to get information is also a great way to get it. A hacker can send a fax or an email to a legitimate user in hopes to get a response containing vital information. Many times the hacker will act like he/she is involved with law enforcement and needs certain data for record keeping purposes or investigations.

Spoofing attack (Phishing)

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.


Your account has been violated !!! - Cyrillic (Windows)
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: PayPal Security Measures
Date: Monday, September 29, 2008 9:35 AM
To: none
Subject: Your account has been violated !!
Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.
Dear valued PayPal member,
It has come to our attention that your PayPal account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.
However, failure to update your records will result in account suspension. Please update your records on or before September 29, 2008.
Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal.
To update your PayPal records click on the following link:
http://www.paypal.com/cgi-bin/webscr?cmd=_login-run
Thank You.
PayPal Update Team
Accounts Management As outlined in our User Agreement, PayPal will periodically send you information about site changes and enhancements.
Copyright 1999-20 PayPal. All rights reserved.
http://201.160.34.201.cable.dyn.cableonline.com.mx/login.php

QUESTIONS

VULNERABILITIES

TYPE	VULNERABILITY
Memory based	Buffer Overflow
	Format String Bug
	Integer Overflows
Time and State based	Race Condition
String based	Session Hijacking
	SQL Injection
	Command Injection
	Cross-Site Scripting
	Improper Use of SSL and TLS
Design based	Directory Traversal

Most people think computer break-ins are purely technical, the result of technical flaws in computer systems that the intruders are able to exploit. The truth is, however, that social engineering often plays a big part in helping an attacker slip through the initial security barriers. Lack of security awareness or gullibility of computer users often provides an easy stepping stone into the protected system in cases when the attacker has no authorized access to the system at all.


S
D
C
X
Z
alt
Matt Murphy

The threat is real

- ✓ ICT is a single point of failure to Businesses.
- ✓ IS Security is Achilles heels of ICT
- ✓ Your security depends on mine and mine depends on yours,
- ✓ Let us come together and fight cybercrime

HOW?

Let us create and manage our CERTs

QUESTIONS