

Cyber Attacks

Prof. Dr. Eşref ADALI

www.Adali.net

Classification of Cyber Attacks

Cybercrime is a crime in which a computer is the object of the crime or is used as a tool to commit an offense.

Active Attacks

Aim to

- Read information
- Change data
- Clear data
- Interrupt activities
- Give damage to the system resources

Passive Attacks

Aim to

- Read information

Internal and External Attacks

Internal Attacks and Fraud

Internal fraud made by member of staff against the organization.

- Payment
- Procurement
- Travel and subsistence
- Personnel management
- Exploiting assets and information
- Receipt

Internal fraud can range from compromising customer or payroll data to inflating expenses to straightforward theft.

Sometimes it's an attack purely for personal financial gain.

External Attacks and Fraud

A person or a group or an organization make attack for

- Read information
- Change data
- Clear data
- Interrupt activities
- Give damage to the system resources
- Blocking of operations
- Financial gain

External attacks aim to financial gain or make damage to system.

Classificaton of Cyber Attacks

Cyber crime against individual

Cyber crime against property

Cyber crime against organization

Cyber crime against society

Cyber Crime Against Individual

Email spoofing

A spoofed email is that e-mail header is forged so that mail appears to originate from one source but actually has been sent from another source.

Spamming

Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters. They do not mean anything.

Cyber Defamation

Someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

Harassment & Cyber stalking

Cyber Stalking Means following the moves of an individual's activity over internet to scare.

Cyber Crime Against Property

Credit Card and Account Fraud

Stealing a credit card or getting card information and use it.

Learning account number and password and use it.

Intellectual Property Crimes

Software piracy : Illegal copying and distribution of computer programs.

Copyright infringement: Using some copyright material without permission.

Trademarks violation : Using a trademark without permission.

Theft of source code : Stealing source code of a program and used it.

Cyber Crime Against Organization - I

Unauthorized Accessing of Computer

Accessing the computer/network without permission from the owner.

- Changing or deleting data
- Voyeurism: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

Denial of Service

When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

E-mail Bombing

Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

Logic Bomb

This is an event dependent program, when the designated event occurs, it crashes some program or delete some file and data or change some data.

Cyber Crime Against Organization - II

Salami Attack

When negligible amounts are removed and/or accumulated in to something larger. These attacks are used for the commission of financial crimes.

Data diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Trojan Horse

An unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Virus attack

Virus is a computer program that can infect other computer programs by modifying them in such a way as to include a copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

Cyber Crime Against Society

Forgery

Banknotes, revenue stamps, mark sheets and some similar valuable things can be forged using computers and high quality scanners and printers.

Cyber Terrorism

Use the computer for terrorism activities. Make some terrorist organization, make some propaganda and demonstration.

Web Jacking

Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Some Numbers about Cyber Crime

Type of Attack	Explanation
Hacking	More than 180 million in 2008
Malicious Software	More than 2,6 million malicious software in 2008
Attacks by Robot (Zombi)	55 million attacks had been done by robots (Zombi)
Organization of Terrorism	More than 90% of the attacks had been done by some organization
Spam	More than 350 million spam in 2008
Phishing	About 400.000 phishing sites in 2009

Affects of Cyber Crime

Economical

Political

Social

Economical affects

- e-commerce : Fake company, fake goods
- e-banking : Fraud

Political affects

- Against to current government
- Terrorism

Social affects

- Defamation
- Forum pages
- Child soliciting and abuse
- Pornography