/ssedcell

Samarth ED Cell

Illuminate Your Way!

Seminar On Cyber Security

CYBER SECURITY AWARENESS

Presented By:- Somapriya Sinha
Trainer & Public Relationship Manager
SAMARTH ED CELL

CYBER SECURITY

Internet security is a branch of computer security specifically related to the Internet.

It is objective is to establish rule and measure to use against attacks over the Internet.

About Cyber Security

- **National Cyber Security Policy is a purposed by Law By Department of Electronics and Information Technology, Ministry of Communication and Information Technology Government of India..**
- **Mission: - To Build a secure and resilient cyberspace for citizen, business and government**
- **To Protect Information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat reduce vulnerabilities and minimize damage from cyber incidents through a combination of structures, people processes technology and cooperation.**

Types Of Cyber Crime

- Hacking
- Software Piracy
- Cyber Stalking
- Spoofing
- Phishing
- Denial Of Service Attack
- Virus Dissemination
- Social Engineering
- Child Pornography

HACKING

The act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed. Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user.

SOFTWARE PIRACY

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Retail revenue losses world wide are ever increasing due to this crime

Can be done in various ways such as end user copying, hard disk loading, Counterfeiting, Illegal downloads from the internet etc.

CYBER STALKING

Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services**. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property,** leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously.

Both kind of Stalkers Online & Offline – have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

- **How do they Operate**
- Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.
- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.
- People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.
- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and adult sites, because of which victim starts receiving such kind of unsolicited e-mails.

- Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
- In online stalking the stalker can make third party to harass the victim.
- Follow their victim from board to board. They “hangout” on the same BB’s as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will “flame” their victim (becoming argumentative, insulting) to get their attention.
- Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.
- Contact victim via telephone. If the stalker is able to access the victims telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.
- Track the victim to his/her home.

SPOOFING

Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges ,, so as to obtain access to the other computers on the network.

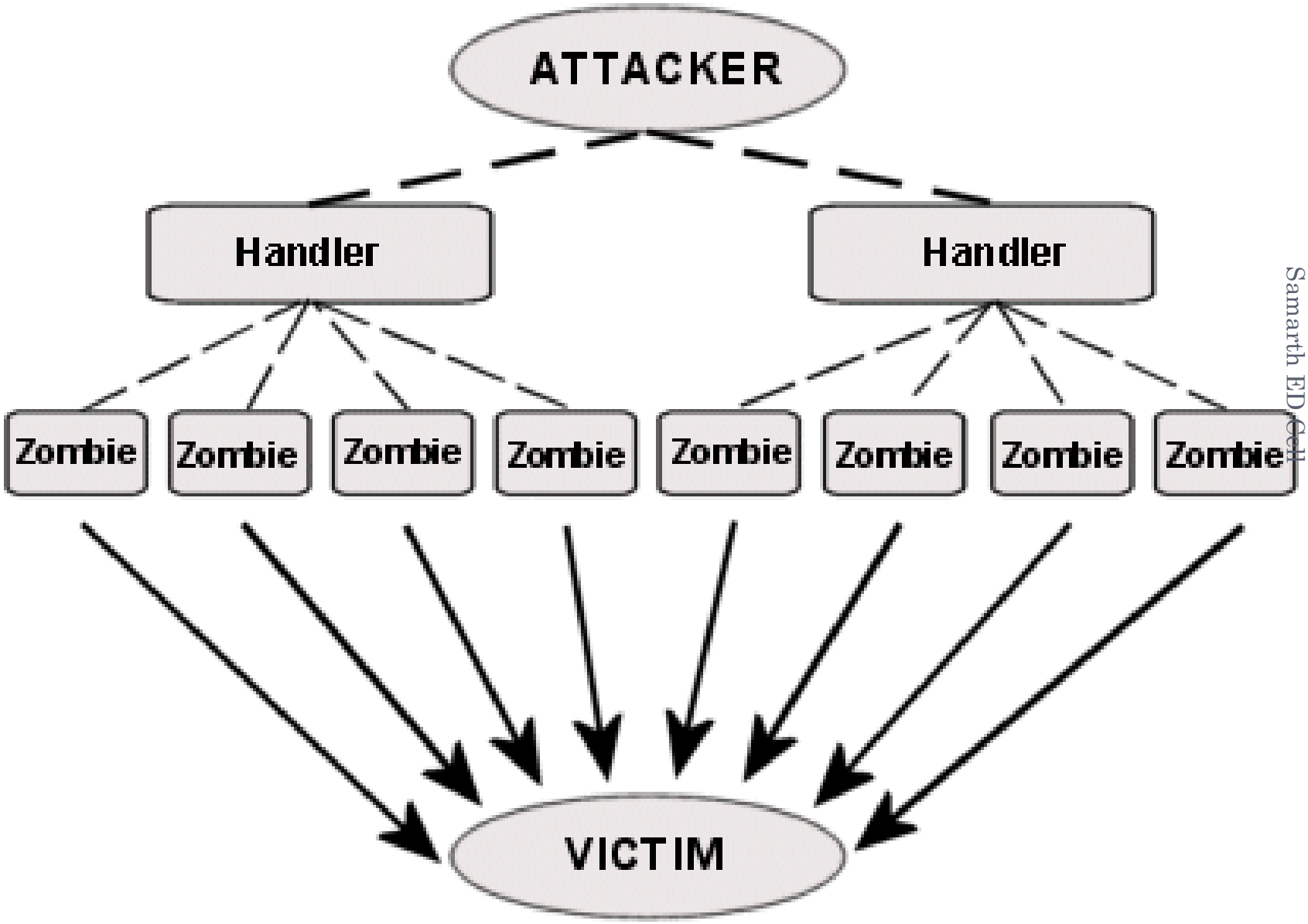
PHISHING

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

Denial Of Service Attack

- This is an act by the criminal, who floods the bandwidth of the victims network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide
- Short for ***d****enial-****o****f-****s****ervice* attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the *Ping of Death* and *Teardrop attacks*, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.
-

Architecture of a DDoS Attack



Virus Dissemination

- Malicious software that attaches itself to other software.
  (virus, worms, Trojan Horse are the malicious software's)
- **Virus/Worms**:- A Software program Design to invade your computer and copy, damage,or delete the file.
- **Trojan Horse:-**Virus that pretend to be helpful programs while destroying your data, and damage your computer, and staling your personal information

Social Engineering

- In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Child Pornography

- The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India .Explosion has made the children a viable victim to the cyber crime. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles.

- **How do they Operate**
- Pedophiles use false identity to trap the children/teenagers
- Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
- Befriend the child/teen.
- Extract personal information from the child/teen by winning his confidence.
- Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address as well.
- Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.
- Extract personal information from child/teen
- At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

Tips for staying safe online

- Don't post any personal information online – like your address, email address or mobile number.
- Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online most people can see it and may be able to download it, it's not just yours anymore.
- Keep your privacy settings as high as possible.
- Never give out your passwords.
- Don't befriend people you don't know.
- Don't meet up with people you've meet online. Speak to your parent about people suggesting you do.
- Remember that not everyone online is who they say they are
- Think carefully about what you say before you post something online
- Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude.
- If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately.


Think before you
CLICK

Any Question?

thank you!

SAMARTH ED CELL

Illuminate Your Way!

Mr. Somapriya Sinha
(Trainer & PR)
/officialsinha

/ssedcell