Rukmini Devi Institute of Advanced Studies

Madhuban Chowk, Rohini, Delhi-110085

(Approved By AICTE &Affiliated With GGSIP University)

DOSSIER

On

Guest Lecture

On

“Quick Heal Solution”

On

April 1, 2014

Ms. Jyoti Arora

Ms. Amandeep Kaur
Chairperson, Literary Club

Prof. Col. (Retd.) Mahander Singh
Director General, RDIAS

FORM A

Proposal:

- **Name of the event to be organized**: Guest Lecture on “Quick Heal Solution”
- **Date:** April 1, 2014
- **Time:** 11:30 am – 01:30 pm
- **Venue:** Lecture Theatre, RDIAS
- **Motivation for the activity:** The session aimed at providing the students fundamental knowledge about virus and antivirus software and will also update students about virus detection, prevention and architecture of Quick Heal Anti-Virus.
- **Organized by:** MCA Department
- **Resource Person**: Mr. Sanjay Ghelani, Technical Assistant Manager, Quick Heal Technologies

FORM B

Part 1

Aim of the event:

The aim of this session was to make students understand the concept of Malware and types of malwares with practical examples & case studies. Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Part 2

Abstract:

The session was taken by Mr. Sanjay Ghelani where he told that Malware includes computer viruses, ransomware, worms, trojan horses, rootkits, keyloggers, dialers, spyware, adware, malicious BHOs, rogue security software, and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses. In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states. Malware is different from defective software, which is legitimate software but contains harmful bugs that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website in the form of a useful or attractive program which has the harmful malware embedded in it along with additional tracking software that gathers marketing statistics.

His presentation focused on the following discussion points:

1. What is Malware?
2. Types of Malware.
3. Top 10 registry Lunch points

4. Case Study & solution
5. Malware Symptoms
6. Malware types
7. History of virus
8. Virus vs. Worm
9. Windows XP vs. Windows 8
10. How to secure Windows XP

Sir explained different types of Malware which are as follows:

Worms- A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

Trojans- A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. The seven main types of Trojan horses are:

1. Remote Access Trojans
2. Data Sending Trojans
3. Destructive Trojans
4. Proxy Trojans
5. FTP Trojans
6. security software disabler Trojans
7. denial-of-service attack (DOS) Trojans

Spyware In another instance of creative software naming, spyware is software that spies on you, often tracking your internet activities in order to serve you advertising.

Backdoors- A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised, (by one of the above methods) one or more backdoors may be installed in order. Backdoors may also be installed prior to malicious software, to allow attackers entry.

Rootkit- Once a malicious program is installed on a system, it is essential that it stays concealed, to avoid detection and disinfection. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator (root) access. Today, the term is used more generally for concealment routines in a malicious program.

URL injectors- This software "injects" a given URL in place of certain URLs when you try to visit them in your browser. Usually, the injected URL is an affiliate link to the target URL. An affiliate link is a special link used to track the traffic which an affiliate (advertiser) has sent to the original website, so that the original website can pay commissions on any sales from that traffic.

Adware- The least dangerous and most lucrative malware, lucrative for its distributors. Adware displays ads on your computer. The Wikipedia entry on malware does not give adware its own category even though adware is commonly called malware. As Wikipedia notes, adware is often a subset of spyware. The implication is that if the user chooses to allow adware on his or her machine, it's not really malware, which is the defense that most adware companies take. In reality, however, the choice to install adware is usually a legal farce involving placing an adware somewhere in the installation materials, and often only in the licensing agreement, which hardly anyone reads.

Sir further explained the difference between Worm and Virus. He said that a worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided.

The malware symptoms below are common signs of a malware infection.

1. PC Performance Problems
2. Interruptions from Pop-ups and Spam
3. Unexplained PC Behavior

At the last, Speaker concluded the session by playing video on malware to understand the concept of malware.

Part 3

Conclusion

It is important for the students to be well acquainted with the applied aspects of the above mentioned areas and should be aware of the intricacies of implementing this technology. Keeping this in mind, the guest lecture was organized for the students to impart them knowledge and make them aware about the technical skill requirement and expectation of IT industries. The session was very informative and included the applied and technical aspects. The speaker explained all the points in detail with demo, case studies, and examples and handled all the queries with expertise. It was a great experience as the guest lecture was highly interactive.

Lecture Moments

Director General, RDIAS felicitating the guest speaker, Mr. Sanjay Ghelani…!!

Mr. Sanjay Ghelani delivering lecture..!!

Students attentively listening to speaker…!!

Time to answer queries..!!