System Security, Spring 2010

Exercise 8

Distribution: 21.05.2010
Hand in: 27.05.2010

Malware – Links

This exercise deals with *malware*. You can find useful information on the following websites (of course you may use other sources as well):

- `www.securelist.com/en/threats/detect` ≫
- `www.spywarewarrior.com` ≫
- `www.avira.de/en/threats/virenkunde.html` ≫

1 Definition

Malware is the short form of Malicious Software. Unfortunately, there is no common understanding of the precise definition of malware. This exercise deals with different aspects of malware and tries to impart knowledge about what malware comprises.

a) Specify at least six different categories of malware. Include everything that might be counted as malware, even if some people or companies disagree with particular categories.

b) Explain each of the categories listed under a) in two to three sentences.

c) Decide for each category under a) if *you* would count it as malware. Explain your decision.

2 Threats

Kaspersky lab is one of several producers of Anti-Virus software. Every detected virus is categorized in an internal database, together with information about the infection process and removal. You will use this index in order to get an overview of the possible consequences of malware.

a) Select an item from one of the Malware Top 20 lists as of April 2010 at:
www.securelist.com/en/analysis/204792116/
and specify its name. Try to find information on your selected malware on the internet. Describe in detail how the malware item works and which potential damage it can cause. (The following tasks all relate to this item.)

b) Is it possible to prevent an infection with the malware? If yes, how can it be prevented?

c) Assume your system has been infected by this malware. How could you detect the infection?

d) How could the infected system be cleaned, if possible at all? Would there be permanent consequences or deficiencies on the infected system?

3 Removal

As usual: prevention is better than detection and removal – also for malware. Nevertheless, it is important to prepare some strategies for removing a potential malware infection.

a) How do you find malware-removal software? Or more precisely: how can you be sure that the malware-removal software actually removes malware and it does not contain malicious software components itself?

b) How do you use malware-removal software? More precisely: Where and how would you install and run the software in order to be sure that the malware is actually removed?

4 Reasons

www.securelist.com/en/threats/detect?chapter=73 describes the connection between the publication of a system/application documentation and the appearance of malware for it.

a) Read the short article and state your opinion on the truth of the statement. I.e, reason why it could be true or why not and draw conclusions from that.

b) Assume that the statement of the article is completely true. Would that imply that documentations should no longer be published? State at least two reasons pro and contra.

5 Prevention and Protection

As already mentioned it is always best to prevent an infection. We now consider the mechanisms that provide the most efficient protection from malware.

a) Give two mechanisms (mentioned in the lecture) which provide good protection from malware.

b) Describe each mechanism listed under a) in few sentences.

c) Argue why each of the mechanisms under a) provides good protection against malware.