Malicious URL

Coming from the Trojan Family

Part 1: Description

A malicious URL is a URL created with malicious purposes -- among them, to download any type of malware to the affected computer which can be contained in spam or phishing messages, or to improve its position in search engines using Blackhat SEO techniques.

Part 2: Infection

Phishing involves sending emails that appear to come from reliable sources (such as banks) and that try to get users to reveal confidential banking information. One of the most widely used tactics is to include a link in the message which, when clicked on, takes users to fraudulent web pages. In this way, users, thinking that they are in a trusted site, enter the requested information, which causes them to fall into the hands of the fraud perpetrator.

On the other hand, Blackhat SEO refers to the use of SEO (Search Engine Optimization) techniques by cyber-criminals to promote their web pages to improve the positioning of their web pages in search engines and to lead users to access them.

A malicious URL needs an attacking user's intervention in order to reach the affected computer. The means of distribution used include spam or phishing messages with links to the malicious site, Blackhat SEO techniques, Internet downloads, and peer-to-peer (P2P) file sharing networks, among other methods.

Part 3: Protection

1. Check the source of information received. Don't reply to any email message that asks for your personal or financial information.

2. When you receive links via email, if you want to access them, type the address into your Internet browser instead of clicking on them.

3. Check that the Web page you visit is a secure site. The web address must begin with https:// and a little closed padlock must be displayed on the status bar of the browser.

4. Check your online accounts frequently to detect any unauthorized transfers or transactions.

5. Don’t forget: banks will never ask you for confidential information through non-secure channels such as email.