Online Security - What is Pharming and how can you Prevent this Online Fraud?

When we look around we are amazed at the speed with which the world is changing. Online fraud techniques such as Pharming and other cyber-crime attacks are at all time high. To overcome such challenges, we need to at least have some basic understanding of these terms. The intention of this informational document is to approach the problem with a solution.

What is Pharming

Pharming redirects Internet users from legitimate websites to malicious ones using a strategy called DNS Cache Poisoning – where corrupt data is inserted into the cache database of a DNS.

The attacker uses several ways to carry out pharming attacks, one of the most popular way is to modify the Host file. The Pharmer covertly hijacks your computer and takes you to a forged website. Your browser may display the legitimate URL, but you will not be on the legitimate server. This, in most cases, is a page that looks identical to that of your bank, financial institution or online shopping websites like, eBay, or Amazon. Here, the attacker seeks your confidential information like credit card numbers, account passwords, etc.

The Hosts fi-le allows storing IP & domain names to speed up sur-fing and avoid consulting a DNS server. So, every time a user enters the address into the browser, the PC accesses the Hosts fi-le fi-rst and, if it -finds this domain name, it takes up the IP address of a website. Now if the Hosts file is modified, the user will be redirected to the wrong website, where the attacker will be waiting to steals the credentials.

To carry out a pharming attack, the attacker typically makes use of the following:

1. A Batch Script to write the malicious IP and domain names onto the Hosts -files.
2. A Joiner to join the batch -file onto another fi-le
3. A Code Obfuscator to help the executable escape detection from anti-virus software.

Phishing vs Pharming

You need to be clear about the difference between Pharming and Phishing. Phishing attacks start with the receipt of an e-mail asking you to visit a website where you may get compromised. Pharming attacks start at the DNS server level where you are redirected to a malicious website.

How to mitigate Pharming attack

Use an anti-virus program which protects you from unauthorized alterations of the Host file is one way. Also, you should regularly patch your operating system and the installed software.

More sophisticated pharming attacks target the DNS server which is usually handled by Internet Service Providers (ISPs). In such a scenario, a user has few options at hand to handle the risk and he can do little against it, except using trustworthy DNS servers.