What is Pharming?

Pharming (pronounced “farming”) is another form of online fraud, very similar to its cousin phishing. Pharmers rely upon the same bogus Web sites and theft of confidential information to perpetrate online scams, but are more difficult to detect in many ways because they are not reliant upon the victim accepting a “bait” message. Instead of relying completely on users clicking on an enticing link in fake email messages, pharming instead re-directs victims to the bogus Web site even if they type the right Web address of their bank or other online service into their Web browser.

Pharmers re-direct their victims using one of several ploys. The first method – the one that earned pharming its name – is actually an old attack called DNS cache poisoning. DNS cache poisoning is an attack on the Internet naming system that allows users to enter in meaningful names for Web sites (www.mybank.com) rather than a difficult to remember series of numbers (192.168.1.1). The naming system relies upon DNS servers to handle the conversion of the letter-based Web site names, which are easily recalled by people, into the machine-understandable digits that whisk users to the Web site of their choice. When a pharmer mounts a successful DNS cache poisoning attack, they are effectively changing the rules of how traffic flows for an entire section of the Internet! The potential widespread impact of pharmers routing a vast number of unsuspecting victims to a series of bogus, hostile Web sites is how these fraudsters earned their namesake. Phishers drop a couple lines in the water and wait to see who will take the bait. Pharmers are more like cybercriminals harvesting the Internet at a scale larger than anything seen before.

Pharming example

One of the first known pharming attacks was conducted in early 2005. Instead of taking advantage of a software flaw, the attacker appears to have duped the personnel at an Internet Service Provider into entering the transfer of location from one place to another. Once the original address was moved to the new address, the attacker had effectively “hijacked” the Web site and made the genuine site impossible to reach, embarrassing the victim company and impacting its business. A pharming attack that took place weeks after this incident had more ominous consequences. Using a software flaw as their foothold, pharmers swapped out hundreds of legitimate domain names for those of hostile, bogus Web sites. There were three waves of attacks, two of which attempted to load spyware and adware onto victim machines and the third that appeared to be an attempt to drive users to a Web site selling pills that are often sold through spam email.