Building a Better Phishing Rod

Phishing is an annoying facet of Internet life these days, but for the most part a "phish" is easy to spot. When you look at the destination of the URLs in the message they expose the phisher. This weakness could be fixed if the phisher combined several techniques, which are described here.

1. `/etc/hosts` trumps DNS

Unix has long had the concept of a 'hosts file' – a file in the `/etc` directory that maps machine names (and domain names) to IP addresses.

Windows now borrows that idea and provides a file called `hosts` in the directory `C:\WINNT\System32\drivers\etc`. By default it contains an entry for `localhost`, but any name can be added, for example;

```
127.0.0.1  paypal.com
```

might be used to fool the PC into thinking that **your** machine is the server for paypal.

It's important to note that an entry in hosts will over-rule the normal process of Domain Name Resolution that a PC would use.

2. Sign My Guestbook

I previously described (http://sagar.org/malbot/) how any one of three million website guestbooks might be subverted, allowing you to easily leave a message for a bot, without needing to hard code anything in the 'bot that would lead back to you or anything you were previously associated with.

My Anonymous Zombie control can of course work both ways. A zombie can leave an encrypted message on any one of 3 million guestbooks indexed by Google and the phisher can go retrieve the message a week later.

3. Gluing the bits together

The other pieces you need to make the perfect phishing rod are:

- Lightweight webserver to install on the persons PC
- Virus to get the webserver on the persons PC and modify the hosts file
- Phishing email claiming to be from PayPal

Lightweight webserver:
The webserver is going to run on the users machine and serve-up a spoof 'paypal' site that allows the phisher to capture the person's details. It will then perform the steps in my previous paper: encrypt and post those details onto a random guestbook.

Virus & Phishing email:
I barely need to mention how the other two points work! Use the 'virus de jour' and attach your own payload in it.

The payload must:

1. Modify the hosts file to make paypal appear as 127.0.0.1 (local loop-back).
2. Install and start the webserver.

4. Collect the money

In order to collect your money, you have to wait a while … the go onto Google and search for your 'bot semaphore' as described earlier.

In a normal phish the authorities could close down your server once the phishing email was recognized. However, in the case of my improved phishing-rod there is no track back to a specific server. The authorities would have to work with the search engine companies to block all searches for Guest Book or somehow trap your bot semaphore.

For you, it's pretty easy to remain anonymous. Use an open WiFi access-point somewhere to do your Google search to download all your captured credit card/SSN/passwords, then go buy your yacht!