INTELLIGENCE NOTE
6/30/2003

Prepared by the
Internet Fraud Complaint Center

"Spoofed" E-mails & Web Sites - A Gateway to Identity Theft and Credit Card Fraud

> *E-mail Spoofing - The forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. Spam distributors and criminals often use spoofing in an attempt to get recipients to open and possibly even respond to their solicitations.*[i]
>
> *IP Spoofing - A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted port.*[ii]

The Internet Fraud Complaint Center (IFCC) is reporting a rise in identity theft, credit card, and Internet frauds due to the fast growing trend of spoofing popular commerce-related web sites. This growing trend is in direct correlation to the continuing decrease in home computer prices, increasing popularity with online auction sites, and the overall lack of technical knowledge of new individuals online. When this type of fraud is reported to law enforcement, the average individual is not aware to include the spoofed web site's HTML code or the full header information from the spoofed e-mail received, thus making the identification and eventual tracking of the perpetrator more difficult.

Spoofing attacks are based upon the ability to make a user believe that they are securely connected to a network address, or receiving e-mail from a specific source, when that is not the case. The problem stems from the fact that the addressing system on the entire Internet is not secure. This creates problems of spoofing in many areas outside web addresses, including e-mail.[iii]

The two main spoofing scenarios seen by the IFCC are 'name similarity' and 'link alteration.'

Name Similarity – One of the more common spoofs occurs when the consumer mistypes the URL they are looking for, or puts the wrong locator at the end. Sometimes the content makes it obvious to the user that the site is not the one they were expecting, but not always.[iv]
For example, the URL for the White House is www.whitehouse.gov. If the average individual is not familiar with the .gov locator, they might enter www.whitehouse.com or www.whitehouse.org. The .com locator will direct the individual to a pornographic web site, obviously not associated with the White House, although the .org locator directs the unsuspecting individual to an official looking web site that mocks the current Presidential administration.

Link Alteration - This attack offers far more gain to the hacker for less actual work, in altering the return address in a web page sent to a consumer to make it go to the hacker's site rather than the legitimate site. This is accomplished by adding the hacker's address before the actual address in any e-mail, or page that has a request going back to the original site. As an example, where the hacker sees a reference to <http://www.mysite.com> they add their own address to it to make <http://hackersite/http://mysite.com>.[v] This fraudulent activity is growing significantly as more people receive e-mail, in HTML format as opposed to plain text. If an individual unsuspectingly receives a spoofed email requesting him/her to "click here to update" their account information, and then are redirected to a site that looks exactly like Ebay or Paypal, there is an increasing chance that the individual will follow through in submitting their personal and/or credit information.

In the past, the IFCC has seen spoofing scams specifically target America Online, Ebay, and Paypal users. More recently IFCC has begun to receive complaints on the spoofing of sites owned by Discover Card, Visa.com, Earthlink, and various other nationwide ISPs. The large majority of the complaints received dealt with spoofed e-mails (as described above). The victims are directed to click on an enclosed link and, in doing so, are transported to a site in order to update their account information for "security reasons." In most instances, once an individual enters his user account and credit card information into one of these spoofed sites, the information is used to commit credit card/bank fraud or identity theft within a short period of time.

Additionally, if the information provided by a victim relates to his/her online auction account, there is a good chance they may find their accounts hijacked, passwords changed, and auctions being run under their username. In such scenarios the perpetrator immediately changes the account's password, thus locking out the actual owner. The perpetrator then uses the victim's positive feedback rating to lure potential bidders to the fraudulent auctions now posted under this account. These auctions are, in most instances, for high end electronics and computers, that will never be delivered once payment is received, thus leaving the initial victim to face the initial fraud charges.

When investigating these spoofing frauds, time is of the essence. In most cases, by the time a victim realizes he or she has been defrauded and files a report with law enforcement, the perpetrator has replaced the spoof site with a legitimate site, or none at all, and has moved on to another hosting service with very little evidence left to track them. In the past, those schemes that were identified early often traced back to web servers here in the United States. Recently however, the IFCC had begun to receive complaints that trace back to perpetrators in England, Italy, Romania, and Russia.

A large portion of the population that receives spoofed e-mail messages ignore and delete them. The IFCC receives numerous complaints from potential victims where no action was taken (information or money lost) after receiving one of these messages. Reporting the 'attempted fraud' by filing a complaint on the IFCC web site is also important in packaging complaints that may comprise numerous "attempts to commit fraud" that represent useful overt acts or lead options . Some of these complaints contain 'cut and pasted' copies of the email but, without the individual including the full e-mail headers or web site HTML code, it is virtually impossible to

track down and identify the perpetrator of these frauds. It is true that the hacker's server must reveal its location in order to carry out the attack, and that evidence of that location will almost certainly be available after an attack is detected. Unfortunately, this will not help much in practice as hackers will break into (or compromise) the computer/server of an innocent third party and launch their spoofing fraud from this victim's hardware. Stolen or hijacked machines will be used in these schemes for the same reason most bank robbers make their getaways in stolen cars.[vi] This scenario was recently seen in February 2003, when a hacker used a University of North Carolina computer system to send spoofed Ebay e-mails regarding verification of personal information. The hacker used a university computer server for more than two hours to collect personal and/or credit information before technicians detected and shut down the scheme.

For those individuals who succumb to this fraud and provide their personal and/or credit card information, they are often only made aware of the scam when they receive their next bank statement. The information culled by these spoofed sites is generally sold or traded across the Internet via chat rooms, newsgroups, message boards, and warez web sites.

---

[i] searchSecurity.com
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci840262,00.html

[ii] University of Wisconsin at Platteville,
http://nw.uwplatt.edu/is/oit/network/reference/terms/s.html

[iii] Articsoft, "Spoofing- arts of attack and defense."
http://articsoft.com/wp_spoofing.htm

[iv] Ibid.

[v] Ibid.

[vi] Department of Computer Science, Princeton University, "Web Spoofing: An Internet Con Game," Technical Report 540-96 (revised 2/97)