

The Enemy Within: Spyware and Identity Theft

by Ilya Lichtenstein for CardCops.com

Identity theft continues to be a massive problem, as information on millions of consumers is stolen from online stores, banks, and small businesses, and later sold on the Internet through private message boards and IRC channels. In particular demand are “full infos” and logins. A “full info” refers to what is traditionally referred to as identity theft- it usually includes someone’s name, address, Date of Birth, Social Security Number, Mother’s Maiden Name, Driver’s License Number etc. In short, this is everything thieves need to register for credit cards, loans, and more in your name. These are usually obtained by employees funneling of customer data for money, or by hackers exploiting vulnerabilities in databases. There are hundreds of vulnerabilities in databases that could easily be exploited, particularly because many websites do not patch their software with the latest updates. Of particular risk are online employment or loan applications, because those contain sensitive data such as social security numbers. This information is often stored in unencrypted form, easily readable by anyone who can access it. Almost all websites that deal with such sensitive data use the industry standard SSL security and claim that “Your information is secure if you see the lock icon in your browser” or something of the sort. This will lull all but the most diligent consumer into a false sense of security, because it implies that your information is encrypted and inaccessible to malicious users. However, SSL encryption, even if it uses 1,024,000 bits only encrypts your information in transit- as it is traveling through the Internet, preventing someone from “sniffing” it and intercepting your information. As soon as it reaches the recipient server, however, it is decrypted and often stored in plaintext form. To a hacker, it makes no difference whether a site uses https or http- the data is no easier or more difficult to obtain. In fact, some of the easiest to hack sites use the strongest SSL encryption- and not much else.

However, many websites, particularly banks and other financial institutions are essentially impossible to hack. Therefore, identity thieves must look to other methods to obtain customer logins and passwords to online banking, PayPal accounts, and more. In the underground, there is a thriving economy in which hackers sell customer login data to carders who then “cash out”, or launder, the money in the accounts. PayPal accounts go for about \$10 each, while customer logins to big banks such as Bank of America go for 1% of the balance. In the beginning, these logins were obtained by phishing, sending fraudulent emails that look like they were sent from the actual financial institution, which directed the victim to login at a fake site that captured login information. However, almost everyone is now aware of phishing scams, and every email list out there has been overspammed with phishing emails. Now, hackers are turning to more devious methods of obtaining those precious logins, and at the same time, taking over your PC.

The most popular tool in their arsenal is the Remote Access Tool (RAT). This is a fancy name for very advanced spyware. While most spyware is made simply to record your browsing habits or bombard you with ads, Remote Access Tools are much more malicious, becoming essentially advanced Trojan horses, software that enters your computer disguised as something else, and then leaves it wide open to anyone who cares

to enter. These Remote Access Tools have a twofold purpose- to steal your personal data, and to transform your computer into a “zombie” or “bot” that is used to attack others.

Usually, a phishing scam can be found simply by looking at the address bar in your browser, and seeing that the URL is different from the banks. Even though the actual login/verification page may look identical to the bank's, but the address of the page is clearly not on the bank's website. However, the pharming scheme can fake the address, and does not require you to open any emails. Every web server is identified by a unique, numerical IP address. For example, the IP address of PayPal.com is 216.113.188.35. If you type “216.113.188.35” into your browser's address bar, it will take you to the PayPal webpage, exactly as if you had typed in the URL. Several servers, called DNS servers, maintained by large companies and Internet Service Providers contain lists that match up URLs like paypal.com to IP addresses like 216.113.188.35. When you type in a URL, the appropriate IP is looked up, and you are directed to it. Through pharming, a hacker gains access to these lists and modifies them. He could change the IP that corresponds to PayPal.com to the IP of his own phishing site. Now, **anyone** who types in paypal.com or visits that URL through a link will go to the phishing site without ever suspecting it, because the URL in the browser's address bar will still read paypal.com. Fortunately, DNS servers are very secure, and are unlikely to be hacked. However, the danger lies closer to home. Tucked away in the C:\WINDOWS\system32\drivers\etc directory is a file called “HOSTS”, which acts as your computer's personal DNS server. It is consulted before any external servers to match domain names to IP addresses. This file can be viewed in NotePad, and can be edited by any program running on your computer. By default, it is empty. But, when edited, it can fool your computer, and even the most experienced computer user that it is on a trusted page, when it really isn't. To see just how powerful manipulation of the HOSTS file is, try adding the following line to your HOSTS file:

```
64.236.16.116 www.ebay.com
```

After saving, open a browser window and type in www.ebay.com. You will see that your browser will open www.cnn.com instead, but the title bar will read “ebay.com”. This is the really interesting part- mouse over any of the links on the page- they are obviously on CNN.com, but they look as if they are from ebay.com. Be sure to change your HOSTS file back – you wouldn't want to visit CNN every time you try to go on eBay. This pointed to the IP of CNN.com, but it could have just as easily been a phishing site that would have gathered your password and redirected you to the real eBay, PayPal, online bank, or anywhere else. The best way to avoid pharming is to look for the “lock” icon in your browser, and make sure the URL starts with HTTPS. Phishing sites will never have this, because valid certificates are only issued to trusted companies that can provide documentation.

A much more dangerous function of spyware is the ability to turn your computer into a zombie completely under the control of its malicious creators or, more often, whoever pays them. On message boards “botnets”, or entire groups of infected computers are be rented and sold, usually to spammers and hackers. Some of the most prized software among spammers, which sell for hundreds of dollars, such as Dark Mailer and Send-Safe is popular because it has the ability to use proxies and relays- in other words, instead of sending spam directly from the spammer's computer, it uses a network of infected computers to do the job. This not only greatly improves sending speed, but also

makes the spammer impossible to find, as all of the tracks lead to the computer that sent the spam- that of an innocent victim. Bots are also used for Denial-of-Service(DoS) attacks, which hammer a website with so many requests that it can no longer function, as is taken down. Organized hackers then demand money from the owners of the website in exchange for the stability of their site.

Unfortunately, even the latest antivirus software, firewall, and patches will not fully protect you from these threats. A popular spyware package that is sold out in the open boasts a scary amount of features. Once it infects someone, it has the ability to view any files on that computer, install other spyware and viruses, modify the HOSTS file for pharming attacks, and much more. Additionally, it is almost completely undetectable. It uses a polymorphic algorithm that constantly changes the signature of the spyware exe file. Because virus scanners detect viruses based on their signatures, the unique “fingerprint” that every executable file has, it cannot be caught by any antivirus programs. Additionally, it utilizes leaks in personal firewall software to bypass most personal firewalls without triggering any alarms. Also, most spyware has the ability to secretly attach itself to other files and execute when that file is opened. Recently, the most popular method of spreading spyware has become Peer-to-Peer file sharing. A hacker simply attaches his spyware to a popular file, and lets it spread on file-sharing networks. When that file is opened, the spyware is installed without the victim ever knowing about it. Because this spyware also features invisibility features, the only way to be truly sure that you are rid of it is to reformat your hard drive and reinstall Windows.

More and more advanced spyware continues to be a looming threat to your personal security and your identity. The best way to avoid this is to only open files from people and websites you trust- for example, a file on download.com will most likely not contain any spyware, when a file on freepornandwarezmoviedownloadzzz.ru is much more likely to contain something malicious. No matter how much security software and legislation advance, these types of threats will never go away. However, with diligence and caution, they can be avoided.