



Wicked Websites

Kelli Tarala

originally printed December 23, 2009

Every where we look, we see companies and people advertising their websites - [www.ComeSeeMy Company.com](http://www.ComeSeeMyCompany.com), www.LookMomImOnTheInternet.com. A website or domain address has become the phonebook, the yellow pages of the Internet. Every business, large and small should have a website. But, have you ever thought about how people get to your website? There are a lot of websites on the Internet. How do search engines like Google and Bing find your website? These search engines rely on Domain Naming Services (DNS) to translate a friendly name such as www.enclavehosting.com to an Internet Protocol (IP) address 67.134.223.73.

Most people rely on the friendly name as opposed to memorizing a numeric address. Most people also trust that the friendly name will take them to the appropriate website. Because of this dependence on friendly names, Domain Naming Services (DNS) are the backbone of the Internet and this leads to the protecting that service that translates between the friendly names and the IP address. This article will discuss some of the security threats facing Domain Naming Services (DNS) and ways that organizations and home users can help protect this critical service.

ICANN and Domain Name Registrars

Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit corporation created in 1998 to oversee Internet-related tasks. For trivia buffs, did you know that prior to the establishment of ICANN, Internet functionality was administered primarily by

one person? A man named Jon Postel at the Information Sciences Institute at the University of Southern California was under a contract with the United States Department of Defense to manage the domain name translation to IP address. It is hard to imagine today that one man controlled the Internet at that time. ICANN was created to assume the responsibility under a United States Department of Commerce contract.

One of the chief functions of ICANN is authorizing domain name registrars. Registrars are companies that are ICANN-accredited to sell domain names based on the generic top-level domains that include .com and .net. An end-user cannot directly register a domain and manage their domain information with ICANN. A designated registrar must be chosen, and companies such as GoDaddy.com, Register.com, and NetworkSolutions.com are all designated registrars. End users must contact them to purchase a domain and website address.

Domain name registrars manage thousands of records. As of September 15th, there were 111 million registered addresses on the Internet. With such a large number of addresses to manage, it becomes easy for criminals to steal addresses or create fake addresses.

Domain Name Abuse

For legitimate businesses, a domain name (website) is a way to market your company online. In the criminal world, domain names



Wicked Websites

Kelli Tarala

originally printed December 23, 2009

are a key part of pretending to be a legitimate and trusting company. These copycat domain names are then used to run botnet and phishing operations to steal information. Cyber-criminals are plundering domain-name registrars around the world to get domain names of legitimate companies. For an inexpensive price, a criminal organization can purchase a domain name, and then use it for nefarious purposes. Criminals are amassing domain names by registering them under phony information, paying with stolen credit cards or hard-to-trace digital currencies like eGold. Criminals purchase domain names of legitimate companies, and install malware packages that commandeer the website for a botnet that will attack and compromise other websites. These are also referred to as zombies.

Domain name registrars have a hard time finding and removing botnets. Cancelling or removing a domain name can be difficult because it is not always clear who the owner of a malicious domain is. There's absolutely a big problem," says Ben Butler, director of network abuse at Go Daddy, an Arizona-based domain-name registrar. Go Daddy, for example, has 36 million domain names under management for more than 6 million customers. It fights a round-the-clock battle to identify domain-name abuse. "We investigate literally thousands of complaints on domain names each week," Butler says. "And we suspend hundreds of domain names per week."

In spite of all these efforts, criminals still slip through the net, in part because registration

services are highly automated, validation processes are insufficient, and the criminals are cagey, determined and technically savvy.

Protect Yourself with a Free Tool: Open DNS

OpenDNS is a service that is available to home users, small businesses, and larger companies, and Open DNS protects Internet connectivity. OpenDNS is currently being used across a wide variety of networks, all with different configurations, but OpenDNS is not software. Open DNS is an Internet service that protects your employees and family from compromised websites as well as protecting your company's Internet connection.

Zero Down Time

Many home users and business users are routed through their Internet providers' DNS servers. If all the Internet providers' customers are using the same DNS servers, everyone will be affected if the DNS servers become unavailable. If the Internet service providers' DNS servers are down, customers will not be able to locate websites unless they have memorized the numeric IP address. Without DNS, the Internet might as well be down.

Since small and medium businesses cannot afford to be offline for any reason, Open DNS provides a distributed global network with redundant DNS servers.

If an Internet service provider is compromised with a botnet or other malicious code, those business configured to use Open DNS will still



Wicked Websites

Kelli Tarala

originally printed December 23, 2009

be online for customers, even if their Internet provider is not functioning.

Filtering and Phishing Protection

Open DNS has the ability to filter out websites that contain malicious code or inappropriate content. With more than fifty categories, OpenDNS organizes the Internet's content for users or businesses to choose a desired filtering level, from "High" to "Minimal." These filtering preferences take effect in just minutes. Some of the categories that can be blocked include Adult Themes, Alcohol, Chat, Dating, Drugs, Gambling, Hate, and Discrimination. This is just a short snapshot of the categories that OpenDNS can block. With a free account, you can manage your home or business network(s) in the Dashboard, setting custom preferences all the way down to the individual public IP address. (www.opendns.com)

Open DNS can also protect your home and business network from phishing attacks. Phishing is criminally attempting to acquire sensitive information such as usernames, passwords by masquerading as a trustworthy entity. Communications purporting to be from banks, popular social web sites, and online payment processors are commonly used to lure the unsuspecting public to fake websites whose look and feel are almost identical to the legitimate one.

Open DNS O operates PhishTank, a site that works by having real people look at suspected phishing scams and verify their illegitimacy.

With no software installation, OpenDNS is a no-risk opportunity to effectively block malicious software and questionable websites. It is an excellent way to prevent malicious software from infected your computers and damaging your company's reputation online as well as around town.

Article reprinted courtesy

