Last Chance for Tens of Thousands of People to Keep Their Internet Access

July 5, 2012 - In April, we reported on a piece of computer malware called DNS Changer that has infected computers all over the world. The program hijacked computers and redirected them to malicious websites without their knowledge. The end result was that for people with infected computers, they saw a lot more advertising, had other viruses and Trojan horses introduced to their operating system and became targets of criminal activity. The good news is that the FBI caught the people behind the program. The bad news is that tens of thousands of computers are still affected and that on July 9th, most of them are going to lose all internet access.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

When the FBI caught the people behind the DNS Changer program, they didn't simply pull the plug on the criminal's computer network. Doing so would have left more than 500,000 computers with no internet access; most of them in the United States. Instead, they replaced the criminal's computers which were used to spread their malware, with clean computers. The FBI has continued to operate this network of fake DNS servers ever since, but that is going to change next week.

As of July 9th, the funding required to operate the FBI's network will dry up and it is scheduled to be shut down. The problem with this is that most of the people who own infected computers, don't have any idea that they have an issue. Their first notice could be when they try to sign on to the internet on Monday morning and get nothing but a blank screen.

Fortunately, there is a way to tell if your computer is infected. Go to http://dns-ok.us and wait for the page to load. If it comes up "green" then you are ok. On the other hand, if it detects a problem you need to visit another website; www.dcwg.org. This is an industry run website with all of the information you need to remove this malware from your computer. But you better act fast. By Monday it could be too late.

ACCESS is advising both consumers and businesses to check all of their computers for DNS Changer immediately. And, as always, it is a good practice to install antivirus software on all of your computers and to scan each computer regularly.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS