the Availability Digest

www.availabilitydigest.com

Will You Have Internet Access After July 9, 2012?

May 2012

The Mayan calendar predicts the end of the world on December 21, 2012. The FBI predicts that up to 300,000 people around the world – many in the U.S. – will lose Internet service on July 9, 2012. If one of them is you, there may not be much that you can do about it except to rebuild your operating system.

How did this happen? And why is July 9th the magic date?

The DNSChanger Malware

The story begins with a well-known class of malware called "DNSChanger." Simply put, DNSChanger infects a PC and changes the IP address of the PC's DNS (Domain Name System) server to a rogue DNS server. It is the DNS server that converts a URL address of a web site (such as www.availabilitydigest.com) to an IP address on the Internet so that the PC can interact with that web site. Without access to a DNS server, a PC browser has no connection to the internet. The only response it will get to a URL request is "page not found."

A valid DNS server is typically operated by an ISP (Internet Service Provider). By changing a PC's routing of URL requests to a rogue DNS server, a hacker can now reroute URLs to a fraudulent web server for whatever purpose he wants. Users will think that they are accessing a valid web site, but in fact they will be accessing a look-alike site that may behave quite differently. For example, if a user clicked on an iTunes icon, he could be diverted to a fraudulent site that purported to sell Apple Products or to a site that infected the PC with additional malware.

The FBI Sting

Following a two-year investigation called "Operation Ghost Click," an international consortium of law enforcement agencies and private-sector partners uncovered a network of rogue DNS servers that were being used in an advertising scam. Estimates are that the network had bilked users out of about $14 million in fraudulent product sales. The hackers were operating as a "legitimate" company under the name "Rove Digital."

The consortium was led by the U.S. Federal Bureau of Investigation (FBI) and included NASA's Office of Inspector General, the Estonian police and Border Guard Patrol, and the National High Tech Crime Unit of the Dutch National Police Agency. In November, 2011, six Estonians were taken into custody by local officials; and the police confiscated several rogue DNS servers located in Estonia, New York, and Chicago that were used in the scam. The United States is pursuing extradition of the six hackers.

According to a study of IP addresses found in the rogue servers, the FBI estimated that the hackers had infected almost four million computers in 100 countries with the DNSChanger malware. 500,000 of these computers were in the U.S. Even NASA computers were hacked.

The version of DNSChanger used by the criminal ring took advantage of a vulnerability in Microsoft Windows. In addition to changing the DNS Server IP address in the infected PC, DNSChanger had network capabilities. If the infected PC was on a small business or home office network, it would search out other devices on the network and would infect them as well. If a router such as Linksys or Cisco was used, DNSChanger had to capability to infect the router if it was configured with the default username and password with which it was delivered. This particular version of DNSChanger also prevented updates to antivirus packages and operating systems.

The FBI set out to notify all infected users and give them guidance (see later) on what to do to disable the malware. By early April, many of the affected users had corrected the problem. However, about 300,000 users may still be unaware that they have been infected. Many of these users - 85,000 - are in the U.S.

Why July 9th?

After seizing the rogue servers, the FBI faced a dilemma. If it simply disabled the rogue DNS servers, four million PCs would suddenly be left without Internet access.

Instead, it contracted with Internet Systems Consortium to set up and operate legitimate DNS servers with the fraudulent IP addresses to temporarily replace the rogue servers for infected users. The FBI provided information to ISPs so that they could redirect their users back to their own legitimate DNS servers.

This move was court-approved, and the FBI was very careful not to give any appearance of government intervention in the Internet. They had no access to any data concerning Internet activity of the victims.

The problem was that the court approved this temporary fix only until July 9th, 2012. Users who have not taken corrective action by then will lose their Internet access.

What to Do?

For users to determine whether they have been infected and, if so, to understand what corrective actions they should take, the FBI has provided detailed information on its web site at www.fbi.gov.

In its document entitled DNSChanger Malware,[1] the FBI gives a detailed description of DNSChanger and methods for detecting an infection. One way is to determine the IP address that a PC is using to access a DNS server. This can be done on a Windows system by entering the command line *ipconfig/all* and looking for the entry that reads *DNS Servers*. This will provide the IP addresses used by the PC to access DNS servers. If an address is any of the following, it is pointing to a rogue server and the computer has been infected:

85.255.112.0	through	85.255.127.255
67.210.0.0	through	67.210.15.255
93.188.160.0	through	93.188.167.255
77.67.83.0	through	77.67.83.255
213.109.64.0	through	213.109.79.255
64.128.176.0	through	64,128.191.255

The referenced document also shows ways to obtain the DNS server addresses for both Windows XP and Apple computers without using the command line.

[1] DNS Malware: Is Your Computer Infected?, *FBI*; November 2011.
http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

Checking wireless routers such as those provided by Linksys and Cisco are model-specific. The manufacturer should be contacted to determine the procedures to detect infection.

To make detection even simpler, an industry-wide team has developed easy-to-use web sites for determining infection by DNSChanger. Multiple languages are supported, and there are one or more web sites for each supported language. These web sites are accessed via the URL www.dns-ok.<country>, where <country> is a country code. For instance, an English web site is found at www.dns-ok.us. Country codes are:

Language	**<country>**
English	us
German	de
Finish, Swedish, English	fi or ax
Dutch, French	be
French	fr
English, French	ca
English	lu
English, Dutch	nl
English	gov.au

German, French, and English versions may also be found at www.dnschanger.eu.

For instance, accessing the .us web site gives an instant indication.[2] A green symbol means that the computer is not infected; a red symbol denotes infection.

Green is Good
Red is Bad

Another site that provides information on detection and correction is managed by the FBI security partner DCWG (DNSChanger Working Group), which includes subject matter experts from many organizations. Its web site can be found at http://www.dcwg.org/.

Unfortunately, there is no patch or fix at this time to remove the infection (though the DCWG web site gives some hints). If a computer is found to be infected, a computer professional or the user's service provider should be consulted. Alternatively, the restore procedures initially packaged with the computer can be utilized.

Summary

Following the successful sting operation, the FBI Assistant Director in Charge of Operation Ghost Click, Janice Fedarcyk, summarized the operation succinctly:

> "Today, with the flip of a switch, the FBI and our partners dismantled the Rove criminal enterprise. Thanks to the collective effort across the U.S. and in Estonia, six leaders of the criminal enterprise have been arrested and numerous servers operated by the criminal organization have been disabled. Additionally, thanks to a coordinated effort of trusted industry partners, a mitigation plan commenced today, beginning with the replacement of rogue DNS servers with clean DNS servers to keep millions online, while providing ISPs the opportunity to coordinate user remediation efforts."

The world economy is truly globalized. By identifying subjects in Estonia who caused a server in Chicago to direct a user in Germany to a fraudulent website in California, the FBI has proven that observation.

[2] Caution – The web site does not ask whether you want it to check your computer. It just does it and displays the green or red result icon.

References

DNS Malware: Is Your Computer Infected?, *FBI*; November 2011.
DNSChanger Malware, *FBI White Paper*
Infected PCs may lose Internet in July, *USA Today*; April 21, 2012.