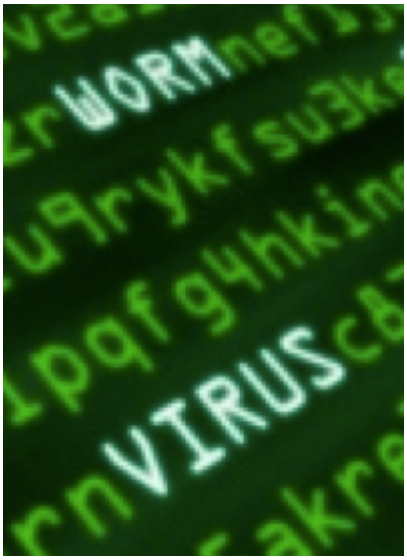
Written by **Dave Bohon** on February 21, 2012

FBI Plans to Shut Down Internet Servers Infected With Notorious Trojan



As reported by PCWorld.com, in November 2011 the FBI shut down a network that a gang of criminal hackers in Estonia had launched to infect servers with the notorious DNSChanger Trojan — a virus that redirects computers from legitimate online destinations to phony websites that launch online ads that generated revenue for the hackers. The Trojan is sophisticated enough to prevent computers infected with the virus from visiting websites with the tools available to remove the problem.

According to PCWorld, the FBI temporarily fixed the issue by replacing "the criminals' servers with legitimate ones that would push along traffic to its intended destination." However, the online news site explained, the "surrogate network was supposed to be temporary — in operation just long enough for companies and home users to remove DNSChanger malware from their machines."

The FBI plans to unplug the temporary network on March 8, and when that happens, "computers infected with DNSChanger will not be able to access the Internet," explained PCWorld. "The malware will send requests to servers that will no longer be online."

The computer tech blogsite Krebs on Security reported that although the FBI has been warning of the impending shutoff and of the importance of companies and individuals to clean up their computers and servers, as of the first of February the DNSChanger Trojan was still active on computers at half of Fortune 500 companies, as well as on PCs at 50 percent of federal government agencies.

As reported by the Krebs blog, "authorities in Estonia arrested six men suspected of using the Trojan to control more than four million computers in over 100 countries — including an estimated 500,000 in the United States. Investigators timed the arrests with a coordinated attack on the malware's infrastructure. The two-pronged attack was intended to prevent miscreants from continuing to control the network of hacked PCs, and to give Internet service providers an opportunity to alert customers with infected machines."

But according to the head of a firm that provides security services intended to remedy attacks from hackers, many companies and government agencies have not been sufficiently aggressive in battling the attack. "Yes, there are challenges with removing this malware, but you would think people would want to get this cleaned up," said Rod Rasmussen, president and chief technology officer at Internet Identity. "This malware was sometimes bundled with other stuff, but it also turns off antivirus software on the

infected machines and blocks them from getting security updates from Microsoft."

While there are efforts to get the deadline extended, if that does not happen millions of computers could go black in early March, warned Rasmussen. "At this rate, a lot of users are going to see their Internet break on March 8," he said.

Experts predict that, even with an extension, completely knocking out the DNSChanger Trojan will take several years. A group formed in 2009 to create a strategy for containing and cleaning up an earlier malicious attack — labeled the Conficker Worm — estimates that nearly three million computers remain infected with that Trojan.

Rasmussen said that given such a projection for fixing the present problem, along with the less-than-proactive approach some companies have taken to ridding themselves of the Trojan, shutting infected servers down in March may be the best option. "I'm guessing a lot more people would care at that point," Rasmussen was quoted by Krebs on Security. "It certainly would be an interesting social experiment if these systems just got cut off."

The FBI has set up a Web page (here) for individuals who think their computers, or a server they use, may be infected by the DNSChanger Trojan.

Experts are recommending that individuals with infected computers have them scrubbed by a professional. For the more tech-savvy individual, once a computer has been scrubbed, a free tool is available for download from Avira.com (or from www.dns-ok.de) that will repair DNS settings on Windows-based computers compromised by the DNSChanger Trojan.