February 12, 2013

HUFF POST TECH

Gerald.Smith@huffingtonpost.com

Microsoft Takedown Busts Up Global Botnet Cybercrime Ring

Posted: 02/06/2013 5:57 pm EST | Updated: 02/07/2013 11:30 am EST

Thousands of computer users around the world received startling news Wednesday when they tried to search online: their PCs were infected and used by hackers to commit cybercrime.

The news came after Microsoft disrupted a network of infected computers Wednesday that was helping cyber criminals commit fraud. In this case, hackers had installed malicious software on computers to steal victims' personal data and hijack search results to charge businesses for online advertisement clicks. By taking down the cybercrime ring, more than 300,000 people around the world will regain control of their computers, Richard Boscovich, a senior attorney at Microsoft's Digital Crimes Unit, said in a blog post.

"What's most concerning is that these cybercriminals made people go to sites that they never intended to go to, and took control of the computer away from its owner," Boscovich said. The malicious software was used "in such a sneaky way that most victims wouldn't have even noticed a problem while the botnet was still operating," Boscovich added.

The infected computers were part of what is called a botnet, or a global network of infected PCs that grows in size as computer users accidentally click on a bad links, files or websites and their computers begin performing automated tasks that help cyber criminals commit identity theft and other types of fraud.

Microsoft received a court order on Jan. 31 to sever all the communications between the hackers and the infected PCs, which were part of the so-called Bamital botnet. On Wednesday, Microsoft – escorted by the U.S. Marshals Service – seized evidence about the cybercriminals from web-hosting facilities in Virginia and New Jersey.

As a result of Wednesday's takedown, thousands of victims whose PCs were infected were temporarily unable to search online, Microsoft said. Their browsers were re-directed to a website that showed them how to clean up their infected computers before they could search again.

The cybercriminals behind the botnet remain unknown, but investigators believe they came from Russia or Eastern Europe because code on the infected PCs contained a Russian phrase that said "I was already here," Boscovich said.

Microsoft worked with the security firm Symantec to help disrupt the botnet. It was the sixth time in three years Microsoft had taken such action to go after cybercriminals.

Microsoft has an interest in combating cybercrime. Its Windows operating systems still dominates the market, and the company is trying to keep its customers secure online.

Last March, Microsoft, joined by a team of United States marshals, raided offices in Pennsylvania and Illinois to disrupt a global network of more than 13 million infected computers that they said helped cyber criminals steal $100 million. In that case, the computers were infected with the so-called Zeus malware that could record users' computer keystrokes to steal usernames and passwords linked to online bank accounts