Microsoft gets legal might to take down spam botnets

September 8 2010, By Byron Acohido

With a judicial assist, Microsoft has perfected a new superweapon to shoot down botnets, the engines cybergangs use to deliver malicious Internet attacks.

The U.S. District Court of Eastern Virginia last week granted a motion that, in effect, gives Microsoft permanent ownership of 276 Web domains once used by the Waledac cybergang to send instructions to hundreds of thousands of spam-spreading PCs.

Cybersleuths and attorneys at Microsoft's digital crimes unit actually decapitated the Waledac botnet in February by persuading District Court Judge Leonie Brinkema to issue a temporary restraining order to take the 276 domains offline.

Brinkema's order was unusual because the owner of the domains could not be reached and thus did not have a day in court to protest, says Microsoft senior attorney Richard Boscovich Sr.

With permanent ownership of the domains, Microsoft now has a proven legal means to take aim at U.S.-registered domains -- including .com, .net, .biz and .org domains -- shown to be conducting criminal activity. "It's open season on botnets," says Boscovich. "The hunting licenses have been handed out, and we're coming back for more."

The Waledac botnet was a major source of spam and PC infections, at its peak in 2009 delivering 1.5 billion spam messages daily. Microsoft

added detection and filtering for Waledac infections to its free malicious software removal tool. But cleaning infected PCs one by one did not stop the command PCs.

By December, Microsoft Hotmail accounts were getting swamped with more than 650 million e-mail spam messages sent out by Waledac. That helped motivate the company to pursue a court order to shut down the command domains.

Even after the botnet's command center got knocked out, tens of thousands of infected PCs continued trying to phone home for instructions. Internet service provider Cox Communications has contacted several hundred of its subscribers by phone to guide them to Microsoft's free cleanup tool.

Lingering Waledac infections pose a risk, says Jason Zabek, safety manager at Cox. "You never know if something else will pop up to try to use it," he says.

Indeed, Microsoft in one recent seven-day period counted 58,000 PCs attempting 14.6 million connections to the 276 Waledac domains it now owns. The company advises using its free Security Essentials program, which will clean up Waledac and many other infections. Meanwhile, it is back at the hunt. "There are dozens of major botnets and hundreds of smaller ones," says T.J. Campana, Microsoft senior program manager. "Botnets remain the backbone of criminal activity."