Microsoft uses law to cripple hacker spam network

February 25 2010, by Glenn Chapman

Microsoft on Thursday said it combined technology with an "extraordinary" legal maneuver to cripple a massive network of hacked computers that had been flooding the Internet with spam.

Microsoft on Thursday said it combined technology with an "extraordinary" legal maneuver to cripple a massive network of hacked computers that had been flooding the Internet with spam.

The software titan's Digital Crime Unit got clearance from a US judge to virtually sever the cyber criminals' command computers from hundreds of thousands of machines worldwide infected with a Waledac virus.

"We decided the best tactic would be to literally build a wall between the bot-herder, the command computer, and all of the other computers -- effectively cutting the umbilical cord," said Microsoft attorney Richard

Boscovich.

Microsoft got a US judge to grant an ex parte temporary restraining order that let the firm erect the cyber blockade without warning bot-herders, masters of the "botnet."

"It was of crucial importance that when we went out to sever the connection between the bot herder and the bots, that severing had to be done without him knowing," said Boscovich, who works in the digital crime unit.

Microsoft drafted a complaint that made a case to the court that the damage to computer owners worldwide, and to the software firm, was major enough to warrant "this rather extraordinary order," Boscovich said.

The mission to take down one of the ten largest botnets in the United States was referred to internally at Microsoft as "Operation b49."

Waledac is estimated to have infected hundreds of thousands of computers worldwide, letting its masters mine machines for information or secretly use them to fire off spam email.

Hackers typically infect computers with malicious codes by tricking owners into clicking on booby-trapped email messages or Internet links that plant viruses.

Bot-herders are then free to hire out botnets for nefarious tasks such as spewing spam or overwhelming legitimate websites with myriad simultaneously requests in what are known as distributed-denial-of-service attacks.

The Waledac botnet was believed to be capable of sending more than 1.5

billion spam email messages daily.

During a three week period in December, Waledac-infected machines sent approximately 651 million spam email messages to users of Microsoft's free Hotmail service, according to the software firm.

The spam included messages pitching online pharmacies, knock-off goods, and penny stocks.

"Three days into the effort, Operation b49 has effectively shut down connections to the vast majority of Waledac-infected computers, and our goal is to make that disruption permanent," a Microsoft lawyer said in a release.

"But the operation hasn't cleaned the infected computers and is not a silver bullet for undoing all the damage we believe Waledac has caused."

Computer users are advised to purge their machines of viruses and make sure their programs and security software are up to date.

US courts allow for hearings to decide whether temporary restraining orders should be made permanent, setting up an unlikely scenario in which bot-herders would argue for their right to reconnect with their machine minions.

(c) 2010 AFP