Hacker 'command' servers seized in US: Microsoft (Update)

March 26 2012, by Glenn Chapman

Microsoft on Monday said that cyber crime "command" servers in two US states were seized in an ongoing campaign to sever online crooks from infected computers used as virtual henchmen.

Microsoft on Monday said that cyber crime "command" servers in two US states were seized in an ongoing campaign to sever online crooks from infected computers used as virtual henchmen.

The software colossus capitalized on laws crafted to fight organized crime groups to obtain court orders to seize servers in Pennsylvania and Illinois being used to control computers corrupted by malicious code.

Viruses slipped into people's computers stole online bank account and password information and relayed it to crooks who have looted more than $100 million in the past five years, according to court documents.

The "worldwide, illegal" computer networks were an amalgam of more than 13 million infected machines referred to as "Zeus botnets" due to the type of malicious code involved.

Zeus malware is designed to log keystrokes typed on computers, watching for patterns that indicate information about online bank accounts.

"A number of the most harmful botnets using the Zeus family of malware worldwide have been disrupted in an unprecedented, proactive cross-industry operation against this cybercriminal organization," Microsoft digital crimes unit senior attorney Richard Boscovich said in a blog post.

The seizure of "command and control" servers by Microsoft employees escorted by police on Friday was the latest move by the industry to cut elusive cyber criminals off from infected computers used to do their bidding.

Microsoft six months ago took down a "botnet" believed to have been used for nefarious activities including spam, stock scams, and sexual exploitation of children, and sued the owner of an online domain used to control operations.

The disrupted "Kelihos" network was an apparent reincarnation of the first botnet Microsoft took down with a combination of legal and technical tactics.

A year ago, Microsoft dismantled a "notorious and complex" network of virus-infected computers used to send billions of email messages daily hawking fake drugs.

That Rustock "botnet" consisted of about a million computers that were

infected with malicious code to let hackers covertly control the machines from afar using "command and control" servers.

Owners of infected computers are typically not aware that hackers are using their devices.

Cutting hackers off from online servers that act as intermediaries, collecting data from and giving orders to armies of infected "zombie" computers, is a creative new tactic in the war on cyber crime.

The raids on office buildings in Pennsylvania and Illinois on Friday involved federal court warrants obtained under different laws, including a racketeering act designed to fight the Mafia.

Microsoft has teamed up with industry allies and law enforcement agencies to destroy spam or crime spewing botnets to defend the reputation and reliability of the software on which the US technology company's fortune is based.

"Microsoft has invested substantial resources in developing high quality products and services," the company said in court documents.

"Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols."

Microsoft resorted to US civil courts to get legal backing to take out the two major botnets last year in a strategy implemented by Boscovich, a former federal prosecutor.

The tactic has been compared to those used by neighborhood watch groups -- ordinary citizens who alert police to suspicious activities.

Hackers cut off from armies of infected computers can regroup and marshal new forces, or adapt viruses to frequently switch command servers or connect, peer-to-peer style, through other tainted machines.

"Identifying command-and-control servers has really come of age in the past year as something that is getting wide attention, especially in the realm of persistent threats," said McAfee Labs senior research analyst Adam Wosotowsky.

"While this surely doesn't put an end to phishing or Zeus-based infections, it should deal a strong blow to botmasters who monetize their infections through thievery," he said.

However, the stepped up US raids could lead hackers to simply relocate to other countries, he added.

"In the struggle between botnets and the security community this is equivalent to a handful of cruise missiles pounding an enemy base," he said.

"It's not the end of the war, but it is a definite statement that our knowledge of the threats has improved to the point where we can target the enemy strongholds."