Microsoft, the FBI and authorities from over 80 countries launch an assault on the Citadel botnets, Reuters reports, taking down "at least" 1000 out of an estimate of 1400 infected networks.

It is believed the botnet stole over $500 million from bank accounts over the past 18 months, as it infected financial institutions including American Express, Bank of America, Citigroup, Credit Suisse, PayPal, HSBC, JPMorgan Chase, Royal Bank of Canada and Wells Fargo.

The authorities do not know the identities of any of the Citadel ringleaders, but believe a "significant blow" was dealt through the takedown.

Microsoft also files a civil lawsuit in the US District Court in Charlotte, N. Carolina, against the anonymous hackers, whose ringleader (referred to in the lawsuit as "John Doe No. 1") uses the handle "Aquabox."

Aquabox probabaly operates from E. Europe, and runs Citadel with the help of at least 81 "herders." Microsoft believes the botnet is run in Ukraine or Russia since it does not attack PCs or financial institutions in those countries.

First seen after the 2011 release of the ZeuS cybercrime toolkit, Citadel combines open source code with additions from multiple virus writers. Its features include keylogging, encrypted malware configuration files, security vendor website blacklisting and invisibility to sites tracking ZeuS.

According to Microsoft "cybercriminals are using fraudulently obtained product keys created by key generators for outdated Windows XP software to develop their malware and grow their business, demonstrating another link between software piracy and global cybersecurity threats."

The company also says “we found that Citadel blocked victims’ access to many legitimate anti-virus/anti-malware sites, making it so people may not have been able to easily remove this threat from their computer. However, with the disruptive action, victims should now be able to access these previously blocked sites."

Go Microsoft, FBI Take Aim at Global Crime Ring (Reuters)

Go Microsoft Works with Financial Services, Law Enforcement and Others to Disrupt Massive Financial Cybercrime Ring