Cybercrime fears remain despite arrests

August 29 2005

Terrorism authorities across the globe have been keeping close tabs on Muslim countries that may be breeding grounds for Islamic fundamentalism, but they are now finding that some of those nations might actually be a hotbed of secular terrorism, namely waging war in cyberspace.

Late last Friday the FBI announced that, together with law enforcement in Morocco and Turkey, it had arrested two people who were responsible for the computer-virus outbreak that hit worldwide earlier this month.

In Morocco the FBI arrested Farid Essebar, an 18-year-old Moroccan born in Russia who went by the screen name "Diablo0," while in Turkey they arrested 21-year-old Atilla Ekici, otherwise known as "Coder." Both men will be subject to laws of their respective countries.

The two were allegedly responsible for creating a number of worms including one called Zotob and another known as Mytob that exploited flaws in Microsoft's Windows 2000 and XP operating systems. A slew of companies and organizations including major U.S. media outlets suffered from the computer-system outages as a result of the worms. Microsoft said the Zotob and Mytob worms have been less damaging that other network worms and viruses in the past, in part because more computer users have become aware of the dangers in cyberspace. Such awareness has led to taking precautionary steps including setting up firewalls, installing anti-virus software and introducing security updates on a regular basis.

Nevertheless, the worms paralyzed many organizations, particularly in North America, and reawakened global awareness of just how interconnected and vulnerable computer systems can be.

"In today's world of sophisticated technology, cyber criminals need very few tools to carry out their crimes. ... The swift resolution of this matter is the direct result of effective coordination and serves as a good example of what we can achieve when we work together," the FBI's cyber division assistant director, Louis Reigel, said in a news release.

Reigel pointed out that in addition to working closely with the Moroccan and Turkish authorities, the FBI also cooperated with the private sector, particularly Microsoft as it was the software giant's program that was targeted by the cybercriminals.

"This arrest demonstrates the value of public-private collaboration -- the first-class investigative work by the authorities and round-the-clock technical and investigative support provided by our internet crime investigations team here at Microsoft," stated Brad Smith, general counsel at Microsoft. He added that "the results (of the arrests) show clearly that cybercriminals will be identified, apprehended, and held accountable for their actions."

Mikko Hypponen, chief research officer at Finnish software security group F-Secure, argued Monday that "Diabl0" had created a number of variants on the Mytob worm since February, but he is not behind all of them.

"There's around 70 known variants of Mytob and practically all of them create botnets of the infected machines. Some of these botnets have been controlled by unrelated groups, such as Blackcarder. And we've found new Mytob variants just yesterday, which obviously are not written by Diabl0. So several people have access to Mytob source code and have been making their own variants," Hypponen said.

Botnets are groups of hijacked computers that all connect to a central control computer and await instructions, such as conducting a distributed denial of service attack, stealing personal information or sending spam.

As such, the arrests in Morocco and Turkey will not make cyberspace more secure, and even the likelihood of the Zotob and Mytob worms being eradicated looks slim.

Microsoft stated that it will continue to ensure Internet safety, namely through technology investments to improve security, partnering with other private companies as well as governments and law-enforcement agencies to develop policies that can be enforced against cybercriminals and keeping customers aware of the potential hazards in cyberspace and encourage them to keep up-to-date precautionary measures to protect them from emerging threats.

Citation: Cybercrime fears remain despite arrests (2005, August 29) retrieved 25 April 2024 from https://phys.org/news/2005-08-cybercrime.html