

Iran To Increase Cyber Warfare Capabilities

Iran will spend one billion dollars to increase its cyber warfare capabilities.

Tehran has embarked on an ambitious plan to boost its offensive and defensive cyber-warfare capabilities and is investing \$1 billion in developing new technology and hiring new computer experts.

Iran has been the victim of a number of cyber attacks in recent years, some attributed to Israel. The most famous attack was by a virus called Stuxnet which is believed, at its prime, to have destroyed 1,000 centrifuges at the Natanz fuel enrichment facility by sabotaging their motors.

...

Last week, the Spanish-language TV network Univision aired a documentary which included secret footage of Iranian and Venezuelan diplomats being briefed on planned cyber attacks against the United States. The documentary claimed that the diplomats, based in Mexico, were involved in planning cyber attacks against US targets, including nuclear power plants.

<http://www.jpost.com/Defense/Article.aspx?id=249864>

Please read the entire article for more important information.

Analysis. I spent most of last week attempting to clean a relatively simple fraudulent anti-virus program off of a business computer. Unfortunately I was not able to and had to clean off the hard drive and start over. The system has been non-functional all of that time. Four business days lost to a program that was only trying to get their credit card information.

I presume that the criminals who invented this program, and hundreds of thousands more like it, are not state sponsored. Imagine what kinds of nasty programs could be produced with the resources of a nation state behind such a group. I'd rather not.

Our nation is woefully inadequately protected against such threats. All of our utilities are computer controlled. If some person could smuggle the Stuxnet into the Iranian nuclear program which, presumably, is not connected to the Internet, how easy is it for some person to smuggle a virus into a telephone company's operations computer system and say scramble their Internet Service Provider system? Or ruin the pumps that supply you with water? Or shut down one of the three electrical grids in the United States?

And I haven't even mentioned an Electro Magnetic Pulse attack yet.

The virus that was contracted by my client was loaded onto the computer from an infected web site. The problem is that lots of web sites get infected and they don't know it until the complaints start overwhelming them. I don't know what the current estimate is for the size of the "botnets" that are in existence right now but I suspect it is in the millions of computers. Their owners don't know they are infected either until maybe they start getting complaints if they can be reached. Anybody who has a static IP address is vulnerable and desirable.

Then there is the Univision documentary referred to in the article. We should also presume that the Russians and the People's Republic of China are making the same kinds of preparations to attack us.

One of the biggest virus creating groups out there is a shadowy group called Russian Business Network. I presume they are part of or affiliated with the Russian Mafia. These are not nice people. They exist in the United States.

Nor are we helping ourselves by running insecure operating systems. Microsoft Windows is not, to me, a secure operating system. Otherwise it would not have approximately 95% of the viruses and other malware in existence written to corrupt Windows. Apple maintains a relatively more secure operating system by keeping a very close hold on the details of the Apple OS. Linux is an open source operating system that is under constant peer review. Security flaws are found generally during the creation of the code for Linux and its utility and productivity software.

I am not for anything that remotely resembles an Internet "Kill" Switch. However, we must come up with a system that allows people infected by other computers to inform the owner of that computer that their system is infected. It is imperative that we find a way to destroy the botnets that are out there and prevent the reestablishment of them. In one famous incident an Israeli company I believe called Blue Rhino set out to gather information on the botnets out there and try to shut them down. Blue Rhino was spammed and Distributed Denial of Service attacked out of business. I started putting the IP addresses of computers that had spammed me on my web site. The next day I got over 1000 spam emails in my mailbox. Such is the power of these people.

It is easy to get the IP address of a computer sending out spam. It is listed in the header of the email which most people don't see. What is difficult to do is to let the owner of the computer know that they are infected and to fix the problem. CERT is probably not the place to deal with such information. The Internet Corporation for Assigned Names and Numbers probably is. Or perhaps a third party located in the Department of Homeland Security that can screen the reports and has the authority to shut down computers until they are cleaned. There should also be an office in the State Department that can deal with computers located off shore.

But the responsibility for keeping your computer clean is yours first. Anti virus programs can be a pain. Some of them really slow down your computer. The alternative is perhaps to become an unknowing spam relay or have your hard drive become a part of a botnet that stores and serves child pornography. If you can, use an operating system other than Microsoft anything (Windows XP, Vista, 7 or server). Go open source where ever possible.