

Matthew N. Wyman

Address 2903 Prospect Pkwy

Durham, NC 27703

Phone (919) 678-0823

Email matthew@northcarolinapcs.com

Technology Alliance - Article 3

Computer Hackers, Internet Crime & Cyber Armies

Computer hackers and hacking in general are on the rise. Chris McNab was right when he said 2004 was the “Year of the Chinese Hacker.” Chris runs Matta, a UK based computer security firm. But 2004 was not alone in this title, 2005, 2006, & 2007 will all go down as Years of the Chinese Hacker, as the Department of Homeland Security, A US Naval Academy & the Pentagon itself were all hacked in America during this time frame.

So why do they do it? Why do hackers of any country hack? It’s illegal and is of questionable morality but still it persists. The reasons are as follows: hackers hack for fun and for profit. They seem to enjoy the challenge of breaking into other people’s computers regardless of it being illegal. Unlike a physical break-in, say to a house, store or bank, the hacker feels safe in the confines of their home or office. Much like automobile drivers, they feel free to express their anger and hostility from behind the safety of their keyboards.

Because of this perceived safety, hacking is on the rise. The fact that hacking has reached even the lofty heights of the Pentagon's Defense Administrator, Robert Gates should signal a real problem. With 150 Pentagon systems broken into and who knows what stolen from them the time to batten down the hatches has long since arrived! The hackers who perpetrated this crime are still considered to be of unknown origin officially, but credible experts say that China's Peoples Liberation Army has hired hackers from the yearly Chinese Hacking Contests that the PLA sponsors. Officials would do well to read chapter 13 of Sun Tzu's the Art of War on Spying as it is required reading for all Chinese Generals.

The primary locations of hackers today are three major countries: China, Russia & the USA, but Britain & Korea are also in the running. All hackers rely on two methods to get into computers. They depend upon weaknesses in Computer Software & weak links in Personnel Security. This is to say that they either find a weakness in your computer or they find a weakness in your employees. Hackers have been known to "dumpster dive" to retrieve information about networks, passwords and usernames as well as targeted "social-engineering." This consists of contacting people who work of the company that is the hackers target and pretending to be someone else in order to get passwords and or login information. Preventing this type of attack means you must educate your employees and keep an eye on what gets thrown away.

The other way hackers get to us is online. This is by far the most common method used by hackers. It involves "Port Scanning," a fancy term for knocking on the tiny doors of your computer. There are thousands of these "doors" that have the potential to be used to communicate with the internet. Fortunately there is a fairly

simple way to prevent hackers from getting into your system, the use of Firewall technology. As with Antivirus, go with a brand name that is not the most popular as hackers focus their energy at breaking into the most commonly used security measures.

As if hackers and computer crime weren't enough, on top of data theft, computer damage, identity theft, financial theft and the national security threats presented by hackers we have another spiky trouble maker, that of Cyber Armies. One of the primary objectives of hackers besides the above mentioned ones is to compromise computers so as to make them work for the hacker. The act of capturing computers has become so common place that the capture systems are called 'Bots.' Hackers will use these Bots to fill the ranks of their Cyber Armies & they are drawing them from the homes and offices all across the Globe but especially in America. When a computer becomes a Bot it may still function as a personal computer or web server. However, in the background or at random times it is woken up by the hacker and made to attack other systems or websites. The owner of the Bot machine may not even suspect that their system has been taken over and is being used for illegal activity. Detecting a Bot machine is tricky, but some tell tail signs are a slow system where you see the hard drive light flickering more often than seems reasonable and internet light on your DSL or Cable Modem that shows activity when your not using the internet.

To complete the picture of the Cyber Army of Bot computers and what they are used for consider the following scenario. An online Casino owner gets a call from an unknown person who offers him a better security package for his web based Casino. After hearing the price of \$10,000 dollars month the Owner says "thanks but no thanks." A week later, the horse races are about to begin and the Casino owner is all set to take

the bets of thousands of customers on whose horse will win. Mean while the hacker who owns and runs and occasionally rents out his Cyber Army of 30,000 computers has just issued a command at an online IRC chat room to his whole army of computers. The command is simple, it says “at exactly 9:45PM Pacific Standard Time go to the following website: www.casinos-are-us.com , continue until 10:45.”

When 9:45PM arrives the hackers Cyber Army wake up and go to the home page of Casino’s Are Us. The arrival and repeated attempt to get to the Casino’s web page by the thousands of Bot computers knocks the web server off line so that all the would be customers are denied access to their favorite gambling casino. The Cyber Army has just effectively performing what is known as a DDoS or Distributed Denial of Service attack. Next time when the hacker calls the Casino Manager goes ahead and purchases the “security package” to ensure that instead of loosing \$50,000 dollars he only loses \$10,000. This is an example of how Cyber Armies are used for Blackmail. Although, deflecting a DDos is beyond the scope of our articles we will be examining hacker prevention in detail in our next article.

The Technology Alliance Newsletter Articles are brought to you by North Carolina PCs online at www.northcarolinapcs.com