Weapons of Mass Destruction

Author: A.Wiederhold

If I asked you if bomb sniffing dogs at airports make sense, no doubt the answer would most probably be "yes". We all know they protect us. If I asked you the same about network security specialists would you be equally quick? There is a new weapon that is dangerous, easy to aquire, and hard to defend against: botnets! Why should you know about them? Read the answer in this article.

A botnet [from "ro-bot" and "net-work"] is a group of thousands of computers running hidden programmes that are just waiting for a signal to attack. The largest botnet discovered in 2004 was made of 25000 PCs. In May 2005 security specialist CipherTrust tracked botnet activity in real-time and found up to 172000 newly infected computers per day! They can attack companies, governments, or network infrastructure. This has been known to the computer science community for quite a while. So what's new about this? The new thing is that this article is on a business school website.

E-commerce and global net-working have become a driver for the development of whole continents. It is also the far-reaching instrument of global westernisation. Although figures for global trade volumes in e-commerce differ heavily [Ecommerce Statisticshttp://www.ecommerce-digest.com/ecommerce-prospects-north-america.html] it seems to have been over $100 billion in 2004 and given the growing computer literacy in Europe and Asia the figure is growing each year. But that is only the tip of the iceberg. The value of a global network lies in its intangibles: free communication, online work, research, knowledge transfer etc. If any densely populated region in the world got disconnected from the internet it would immediately enter a state of emergency. Can you think of a large and heavily networked economy in the world that sees itself as a target of terrorists? I can.

Now that we are beginning to understand the threat let's understand the attack. On hundreds of thousands of computers around the world security holes have been used to install software without the permission or even the knowledge of their owners. This software is inactive, waiting for a command. If that command is given, the computer might generate a simple and perfectly legitimate network request. It would for example try to download a file from a webserver in an foreign country. There is nothing suspicious about that, neither on the attacker side nor for the victim. But if 25000 computers do the same thing, the server will go out of service. This is called a DOS [denial of service] attack, and has been successfully carried out many times in the recent past. Needless to say that Microsoft was repeatedly a victim. But also smaller companies have become

targets.

What makes botnets so dangerous is the fact that they are big enough to congest whole internet backbones. They don't target a single company, they can attack the internet infrastructure of a whole region. The internet is by definition built to re-route information if a certain path becomes unavailable. How convenient for botnets: their attack will be re-routed to jam the backup routes.

So far, service providers and regional networks have seen sporadic attacks that didn't last long. But as technology spreads into the far corners of the world so may the knowledge that a PC and a well-paid hacker can be a far more powerful weapon than an airplane on September 11. If well-constructed it only takes a PDA or a mobile phone with internet connection to trigger a botnet anywhere in the world to attack any target. The laughing villain that presses a button on his WAP-phone or PDA and puts a whole country out of business is no longer material for James Bond movies. It is reality.

Botnets will undoubtedly become the weapons of mass destruction in the virtual world. They can disconnect businesses and customers, and whole countries. Education, tele-work, virtual research teams, weather and news information, stock markets, countries that depend on outsourcing [e.g. India, China, but also Great Britain, Germany, and the US], all are affected by botnets. And how could some of us live without emails, chats, and online games?

It is most disturbing that this threat is known for years and yet nobody seems to tell the business community anything about it. If NASA gets hacked or Microsoft is offline because of a DOS attack they are in the news briefly. But the bigger picture remains in the dark. Business schools need to educate the next generation of managers and decision makers so that they are prepared for the future. We understand that bombs on planes are bad for business. Botnets and network security should be something we understand equally well.