



Challenges of Securing Information.

TODAY'S SECURITY ATTACKS

For the IT security professional it is a 24-7 job fighting cyber criminals that want to inflict pain on computers, networks and their users. It is a job that requires constant vigilance and many security firms run network monitoring centers to keep an eye on their customers' networks and the shifting tide of computer vandalism and crime. It is like trench warfare.



Mission Assignment: MP1-1











Type: Individual - Blackboard Discussion Board Forum: **MP1-1: Today's Attacks**

Resource: Internet, personal experience, assigned reading.

Description:

Virtually everyone that is connected to information technology has at one time or another been affected by cyber criminals; 4 out of every 5 Internet users, 14 adults per second. Realistically, there are many more types of "attacks" than there are devices and these attacks are often very complex.

The table below identifies a few of the most recent attacks. This assignment will require that you define the attacks that you are assigned in your Blackboard discussion group. The entire list of attacks is shown in the table below, some suggested discussion points will be detailed in the discussion board.

	Email
	Mac attack
	Medical devices
	Credit cards (and other personal ID breaches)
	Car hacking
	Unpatched servers (data/code breach)
	Wireless networks
	Pre-hacked imported devices
	Mobile devices (cell phones, tablets, etc)
	Internet attacks/fraud

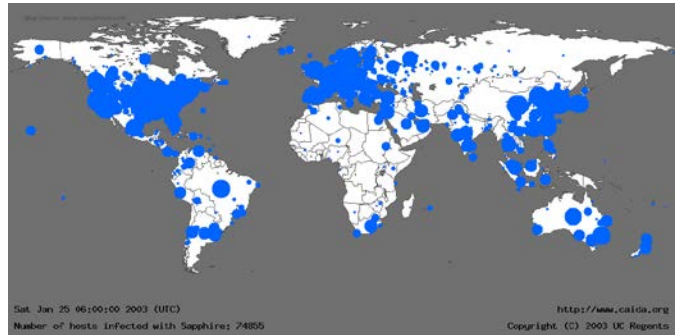
DIFFICULTIES IN DEFENDING AGAINST ATTACKS

It is a challenge to everyone that works (or plays) on computers, to **not** have a worry about security. Of course you can almost reach 100% security if you never connect your computer to a network (wired or wireless) and never attach a removable device to that computer.

Because of the number of potential security attacks and the speed by which they happen, it is very difficult to manage security.

SPEED

We are a global economy. Attacks can rapidly spread to thousands of victims in just minutes – and it is possible for this to happen even without human intervention.



SOPHISTICATION

Anything that is complex is difficult to understand. Complexity, with regards to computer attacks, makes it difficult to detect and defend against these attacks. Many modern attacks are made to look legitimate, in other words trusted by your computer. Sometimes attacks enter a computer hidden inside a legitimate transaction, for example. In some cases computer attacks morph themselves so that computer anti-viruses will not recognize their "signature".



SIMPLICITY OF ATTACKS

Even you can be an attacker. Is it an instinct? Not really, you still have to learn the technique. In fact, if you know how to hack computers ethically, you will likely be able to prevent attacks on computer systems and networks. There are a few well known resources that will help you become an ethical hacker.

Click on the images/links below to check out these resources.



[HTTP://WWW.BACKTRACK-LINUX.ORG/](http://www.backtrack-linux.org/)



<http://www.metasploit.com/home/>



[HTTP://WWW.EXPLOIT-DB.COM/](http://www.exploit-db.com/)

QUICK DETECTION OF VULNERABILITIES

This means more "Active Attacking" vs. passive attacking. Active attacks are attacks on systems that have a known vulnerability, which may not have a fix until the computer gets "updated".

Then, there are zero-day attacks. This is when a vulnerability of a system is discovered by the bad guys before the security community (the good guys) can fix it.

Click on the image or link below to read an article relating to a “critical” patch released by Microsoft that directly relates to this issue.

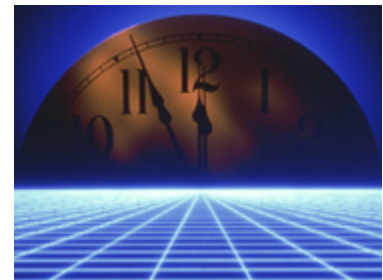


<http://blogs.zdnet.com/security/?p=2853>

DELAYS IN PATCHING PRODUCTS

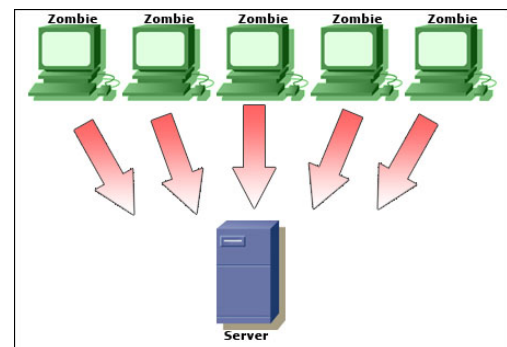
Writing product updates immediately for every single malicious attack possibility is impossible.

Consequently, updating or patching a product has delays, thus allowing attacks to penetrate systems.



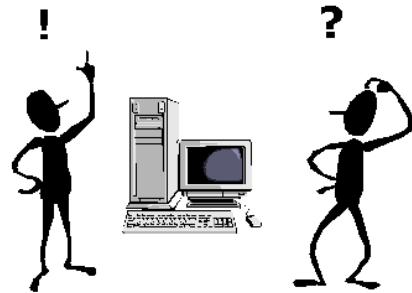
DISTRIBUTED ATTACKS

When attacks come from another computer, the attacking computer may have other computers working with it. When this happens, it is difficult to block the attack by blocking the source.



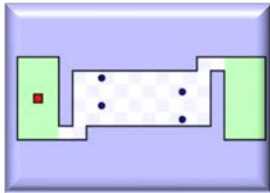
USER CONFUSION

An uneducated guess can lead you to make the wrong decision regarding security.



Adapt the machine to suit the cognitive characteristics of the human being using it.

Click on the Game Link image below to play a matching game to review the above topics.



[HTTP://COURSECONTENT.NTC.EDU/CIT/HUSBAND/POIS/LP1/M12-GAME.HTML](http://coursecontent.ntc.edu/cit/husband/pois/lp1/m12-game.html)