The Truth About Cyber Terrorism

The new 'terror' facing the world today is that of Cyber Terrorism. Airplanes being hijacked from a remote location by a hacker who has breached the cockpit control system, power grids being shut down by a hacker who was paid by a terrorist organization, attacks on banking systems worldwide. School buses full of children having head on collisions because a hacker was paid to alter the pattern of an intersection stoplight. These threats, however unlikely they may seem, are nonetheless real and must be eliminated.

The daily threat, Identity Theft.
According to the FTC, more than $437 billion has been lost to consumers due to online fraud in 2003. The US alone reported losses totaling more than $1.07 billion. It is important to note that when corporations lose money, the consumer suffers from increases in cost of services.

Of all Operating Systems and browser types the Windows based programs are the most vulnerable to hacker attacks. As of February 2005 64.9% of the browser types used and 62.0% of Operating Systems used were Windows based Internet Explorer and XP. At any given moment in time, a hacker can be going through your computer, gaining access to all of your vital personal information. Identity theft is unlike any other common theft because the chances of the perpetrator being caught and convicted are slim. Your entire world can be altered with a keystroke. Banking accounts, credit card accounts, social security numbers, insurance policies.

The answer is not to stop putting your information on a computer, the solution is Artificial Intelligence based software that completely eliminates the chance of a hacker accessing your information.

ARTIFICIAL INTELLIGENCE

Function: *noun*
Date: 1956
1: the capability of a machine to imitate intelligent human behavior
2: a branch of computer science dealing with the simulation of intelligent behavior in computers.

Artificial Intelligence, or A.I.,is the most powerful security available. Unlike other 'anti hacker', or 'anti virus' programs, our A.I. based programs have been 'taught' how to countermeasure hacker attacks. With every attempted breach in the network, the A.I. data base is expanded. It is software that thinks like a human being, allowing it to react like a human being. When an intrusion of any type is detected it is eliminated before it can gain access. Housed on state of the art " Eihwaz" servers, our main A.I. " Aries" is knowledgeable in every form of anti hacker countermeasure available. "Aedan", the A.I. that runs on the network is in constant communication with Aries through M.O.M (Missions Operations Manager).

AedanSafe Products

The AedanSafe product line was created due in part to the inefficiency of all other products currently on the market as well as the inefficiency of Windows. Current products on the market cannot prevent malicious code from entering the network. It is found only after it has breached the network and wreaked havoc. It is then 'deleted' putting it in what is called the deep cluster zone. Viruses in the deep cluster zone can still replicate. Current products find malicious code by their 'definitions'. Aedan locates malicious code based on its activity, it monitors the tasks running, executed functions, modified and newly installed applications. Aedan locates viruses, spyware, and other types of dangerous xcodes and then kills the process of the virus if it is running, destroys the data, then reports to Aries if it needs any information on countermeasures and advanced hacker attack. In a world where businesses and citizens cannot afford to have vulnerabilities on their network, a product had to be created that not only eliminated the problems currently on the network but also prevents future problems from occurring. When companies care more about their 'bottom line' than the quality of service they provide, it is time for a new

company to emerge. A company that understands the need to be secure without pricey software that has to be updated regularly or purchased on a yearly basis.

All products are AI based security software for every sector. Personal, corporate, educational, and government. Aedan simply has to be installed on the computer in order for it to remove, detect, and prevent all forms of intrusion. Aedan never has to be updated, a new version does not have to be purchased every year, and most importantly, it works.

Current industry standard for the 3G phones is to use a mobile firewall. A firewall can be shut down by a firewall killing tactic or 'nuker'. A nuker sends multiple oversized IGMP packets, tries an Out of Band nuke or OOB, floods the target ip with oversized ICMP packets and then kills the firewall by connecting to every port simultaneously. For powerful computers, like the Pentium 3, your firewall uses your processor as a resource to resist against this tactic, causing your operating system to reboot your computer , accomplishing the goal of the hacker. A mobile device does not have the same capabilities and processing power as a computer and these same nuking tactics will severely damage the hardware on any mobile device if this attack is launched, making it dangerous to have a firewall on a mobile device.

Aedan Embedded devices will run on all mobile operating systems protecting the user from viruses, trojans, and other java, XTS, WinCE, PalmOS, and IC2 user environments that viruses are coded to emulate.

All Aedan products are coded so that ARIES recognizes each individual Aedan disk, very much like a parent would recognize their own child, thus eliminating any chance of cracking or hacking our products. When an Aedan product is registered it can only be used on the computer it was registered with. A copied version of Aedan will not be recognized by ARIES. In the event that the registered user needs to install Aedan on a new computer, a new code will be issued and the old eliminated.

AedanSafe Products include:
AedanSafe@HOME
AedanSafe@WORK
AedanSafe@SCHOOL

Aedan will be sold for $39.95 (Windows ALL)

Guardian Angel

Guardian Angel is a program aimed at government use. This program will eliminate any chance of a hacker breaching the security of a Nations infrastructure. With technology, such as that used on the GlobalHawk, enabling remote access to cockpit controls, GUARDIAN ANGEL is aimed at protecting all military, private, and commercial aircrafts from outside parties wishing to gain remote access to cockpit controls, Guardian Angel also protects the information feed of communication for military and private security to prevent weapons defense systems on aircraft carriers, nuclear submarines, and other naval vessels from being misguided to a false target (friendlies), by terrorists.

BlueSphere

BackSpace2 also provides state of the art 'anti hacker' live disks to those businesses wishing to learn how to secure their network. BlueSphere is a unique and evolved program powered by Artificial Intelligence that is used for the training and certification of IT Security Professionals. Upon completion of the certification, BlueSphere is then used as the company's network security program, the worlds first and only A.I. powered Intrusion Prevention System.

BackSpace2

With BackSpace2 you are closing the windows of the past and opening the doors of the future. This is a new world with new threats. The team of BackSpace2 is comprised of people who care about security in a world where terrorists feel at home. We are not interested in using technical terms to confuse you or run circles around the problem. It is our goal to eliminate the threat of cyber terrorism. This can be done with Artificial Intelligence and you, the consumer. If you would like more information on products and services please view our website at WWW.BACKSPACE2.COM or email us at operations@ariesoft.net

Thank you and have a Powerful Network!