Title:
Security A 21st Century Concern

Word Count:
504

Summary:
Security is of major concern in today's world as the world has become increasingly complex and easily accessible, especially via the internet and email. One of the most important issues facing people regarding security today is in regards to computers. Most of the security issues in relation to computer viruses and worms, Trojan horses, and the like, are geared predominantly to the PC consumer market.

Ranging from running adware to hijacking browsers, infecting computers w...

Keywords:

Article Body:
Security is of major concern in today's world as the world has become increasingly complex and easily accessible, especially via the internet and email. One of the most important issues facing people regarding security today is in regards to computers. Most of the security issues in relation to computer viruses and worms, Trojan horses, and the like, are geared predominantly to the PC consumer market.

Ranging from running adware to hijacking browsers, infecting computers with malware and spyware programs that run massive spam emails, act as servers, completely overtake computers, steal personal information including social security and identity numbers, personal residence information, age, demographics, as well as credit card and banking information, to running pornographic material and ads, the amount and variety of spyware and adware threats that pose security issues to computers, have compounded in the last few years, exploding the increase of security violations.

One of the most prevalent penetrators through computer firewalls and security systems, is the computer worm. Defined in the Oxford dictionary as a self-replicating program able to propagate itself across network, typically having a detrimental effect. Computer worms primarily replicate on networks, but they represent a subclass of computer viruses. With the wide variety of computer

worms and viruses, researchers differ on the exact definitions of computer worms.

The network-oriented infection strategy is indeed a primary difference between viruses and computer worms. Moreover, worms usually do not need to infect files but propagate as standalone programs. Additionally, several worms can take control of remote systems without any help from the users, usually exploiting a vulnerability or set of vulnerabilities.

Each computer worm has a few essential components, such as the target locator and the infection propagator modules, as well as a few other non-essential modules, such as the remote control, update interface, life-cycle manager, and payload routines. The worm needs to be able to find new targets to spread rapidly on the network. Most worms search your system to discover e-mail addresses and simply send copies of themselves to such addresses, a highly convenient system for attackers looking to break into a corporate firewall. Most corporations typically need to allow e-mail messages across the corporate firewalls, thereby allowing an easy penetration point for the worm. Many worms deploy techniques to scan the network for nodes on the IP level and even "fingerprint" the remote system to check whether such a system might be vulnerable.

Another important component of a worm is remote control using a communication module. Without such a module, the worm's author cannot control the worm network by sending control messages to the worm copies. An update or plug-in interface is an important feature of advanced worms to update the worm's code on an already-compromised system.

The attacker is interested in changing the behavior of the worm and even sending new infection strategies to as many compromised nodes as possible. The quick introduction of new infection vectors is especially dangerous. Many worms have bugs in their life-cycle manager component and continue to run without ever stopping.