Chapter 35

LIMITING DAMAGE

INTRODUCTION

Why are current Internet security measures ineffective in detecting unknown malicious network-enabled applications? Each of the existing security measures, firewall, router, Anti-Virus etc., plays a vital role in protecting personal or business information. However, they are not effective against new and unknown network-enabled malicious applications, which are the fastest growing group of malicious applications [1].

Anti-Virus software can detect only known malicious applications, while the most damage is done by new and unknown programs. Even though Anti-Virus software manufacturers claim that it detects both known and unknown malicious programs, experience suggests otherwise [1].

The truth is that in a vast majority of cases Anti-Virus software can detect only known malicious applications, usually after damage has been done to thousands and some times millions of computers. If Anti-Virus software were truly capable of detecting unknown malicious applications using profiling – heuristic analysis, then there would be no need for a database. In fact heuristic analysis (profiling) is not reliable and in general is completely powerless against those unknown malicious applications that do not damage data but steal information or paralyze the network (network-enabled Trojans, worms, spyware etc). The recent worm barrage is a graphic example of Antivirus software's inability to deal with the "new and unknown [1]."

Many malicious applications designed to steal information will never be detected by Anti-Virus software. A worm attack is so massive that the assailing worm will inevitably be detected, sent to the Anti-Virus lab and eventually added to the database [1].

At the same time, today's profit-driven hackers use customized attacks against individuals and businesses. Customization means that a hacker designs a malicious application for a specific attack. As a result, this malicious program could exist in a very small number of copies (some times just in a single copy) and therefore has virtually no chance of being discovered by the user and sent to an Anti-Virus laboratory. Thus an unknown malicious

program that shows no symptoms and does not propagate can exist through the life-time of the computer completely undetected stealing information even from the apparently most secured environment [1].

APPLICATION FIREWALLS

An application firewall requires an expert to be effective. But even for an expert without specialized tools (essentially an Anti-Virus laboratory) the decision will still remain an educated guess [1].

Even if an application firewall is able to stop the most sophisticated test, in real life, it has a low chance to prevent a malicious program from operating, because it relies solely on the end-user expertise. As a result, a malicious program is very unlikely be stopped unless it is called "iamreallybadatrojan.exe" and the user is warned in advance to lookout for it [1].

APPLICATION FIREWALLS WITH CENTRALIZED MANAGEMENT CONSOLE

An application firewall with a centralized management console allows an administrator to create a list of pre-approved applications for every computer on the network. As a result, in theory any application that is not approved will not be able to work [1].

However, realistically the centralized console will only lock *.exe files while dynamically linked libraries, representing the majority of executable code will not be controlled. Internet Explorer, for example, will have its *exe file locked, however its components (of which there can be as many as 60), will not be controlled [1].

Even though an option to lock components might be available, continued and constant updates of the operating system and applications make it impractical. An application firewall with a centralized management console creates an extremely restrictive environment for the end-user that can negatively affect productivity. Application firewalls are also not affordable for a vast majority of businesses due to the costs of their administration [1].

Perimeter firewalls or routers do not protect against attacks originating within a local network. The best corporate firewall or the best router will not prevent a malicious program from sending data outside the corporation, because the malicious application can use the same client type Internet connection as legitimate applications, such as Internet Explorer, messengers etc. [1].

TRAFFIC MONITORING INTRUSION DETECTION SYSTEMS

Similarly to perimeter firewalls traffic monitoring, intrusion detection systems are ineffective in detecting malicious applications. Why? Because, they do not know which application sends data, legitimate Internet Explorer or one of its malicious components [1].