Global Information Assurance Certification Paper

Make All Your Internet Traffic Play in the Sandbox

Jonnie Long
November 22, 2000

A new virus signature file was released today for the award winning anti-virus software on your company's servers, desktops and Internet gateway. You upgraded the signature files on all servers and gateways, pushed the signature files to all desktops and verified that the scanning engines are the most up-to-date versions available. Surely the company's network is now secure and you can begin to tackle the myriad of other tasks that keep an IT department busy, at least until new signature files are released in about two weeks.

But is your network really secure? What about the Excel file that Bill in accounting just received from a partnering firm. The anti-virus software checked the file and the macros it contained before Bill opened it and deemed the file to be safe. Then there's Sam in sales, he receives dozens of email messages every day with attachments that the anti-virus software scans before downloading. The attached exe, zip or other files are safe to use after being scanned by the anti-virus software aren't they? Or what about Jill in marketing, she is doing research on the Internet for that proposal due next week and there is nothing to fear from browsing the Web, so long as you don't download any files.

Unfortunately, Bill, Sam and Jill were all victims of the newest threat to corporate networks, malicious Active Content sometimes called Internet mobile code. Malicious active content can enter the company's network through email attachments in the form of executable files, zip files or Microsoft Office documents with macros. It can be downloaded by users from the Internet as innocuous applications (such as screen savers) and even by simply viewing HTML Web pages or emails that contain invisible hostile code (Java applets, VBScript, JavaScript and ActiveX controls). The malicious code can be used to change or delete files and send passwords and other information to parts unknown. It can provide a back door for remote control of the affected systems and even launch attacks against other systems. In short, the malicious code can do anything that the desktop user can do, since it is running with all the rights and privileges of the desktop user. And all of this malicious active content can enter the company network under the watchful eye of the up-to-date anti-virus software.

According to Dave Kroll, director of corporate marketing for Finjan Software, "Most people think that when they're surfing the web they are visiting other web sites. Actually, those web sites are coming to you. Those graphics and auto-executing code are running in your system's memory and are capable of performing any function on your PC that your can. This is what most users don't clearly understand."(1)

Why didn't the anti-virus software stop the malicious active content and most importantly, what can be done to keep your company's network secure today and tomorrow?

Let's look at the anti-virus software available today. Traditional antiviral software take a reactive approach to identifying viruses, worms and Trojan horses by matching file patterns or binary signatures to a database of known virus signatures.(1) Therefore, the anti-virus software can only identify viruses **after** an infection has occurred and the database has been undated to

include the new signatures. It can react to a known virus signature but bypasses any file not included in the signature database. That method worked well in the past when viruses replicated fairly slowly and anti-virus companies had days in which to update signatures before the viruses spread to epidemic proportions. In 2000, new viruses and worms such as LoveBug spread around the world in hours, not days, far too fast to be halted by traditional anti-virus software.(4) Additionally, if a known virus, or Trojan horse file has been compressed by one of the hacker friendly packer programs, the binary signature is changed during compression and the new file can bypass the anti-virus scanner. (2)

So why don't we just reject any email with attachments, turn off all ActiveX, Java, VBScript and JavaScript functions in our email and browser programs, disable macros in Microsoft Office applications and protect ourselves? A company could do that and protect themselves, but how long would it remain competitive? The vast majority of Internet code is very useful. Without email attachments, organizations would be unable to exchange electronic documents, presentations, and spreadsheets. Without active content like scripts, Java applets, and ActiveX controls, Web sites would be reduced to static text and graphics.(5)

The Solution: Sandboxing Technology

The Sandbox techniques are proactive and stop the malicious actions of Internet code before they occur.(3) The sandbox allows active content to be run in a controlled environment, creating an impenetrable barrier between the Internet code and the Windows operating system. The sandbox tracks all active content downloaded from the Internet whether from email, Web browsers or directly downloaded using FTP. The sandbox surrounds the active content and intercepts all requests for system resources or services. It then compares the request to a set of policies or rules established by the IT department and will either allow or deny the service request accordingly. This set of rules is the core of the sandbox technology and determines what active content is allowed to do and what cannot be done. The behavior of the active content will determine whether it is allowed to function or stopped dead. By default the sandbox will deny every request for service from the Internet code that is not specifically allowed. In this way email clients, Web browsers, FTP programs, chat clients, Microsoft Office applications and other programs can be run with all of the beneficial features of the active content enabled and still be protected from hostile or malicious actions.

Since the sandbox software is making decisions for services based on a predefined set of rules, new, unknown viruses, Trojan horses, Java applets and so forth have no effect on the ability of the sandbox to protect your system. If the access control policy does not allow an executable email attachment to create a file in the Windows system directory, it will stop the Happy'99 virus from working today and stop any virus from doing the same thing in the future. Even if the virus hasn't been discovered yet.

This access control is what makes the sandbox technology so proactive. Since the sandbox is proactive, it is not dependent on frequent updates to remain effective, nor does it need to be concerned with new technology. Even if someone invents a new programming language to replace Java, since the sandbox is denying all service requests not expressly permitted, any new programming language would be denied also.

The sandbox software should reflect the access control policies of the company security policy and can be as broad or granular as desired. Different policies could be assigned to individual people, groups, resources and even types of active content.(4) For example, if a company has critical data they want to protect, a policy could deny access to this data from a Java applet or ActiveX control. The user would have full access to the data using their usual programs, only the Java applets would be denied this access. Another policy could prevent a browser from making sensitive registry changes or deny script files from reading mailing lists and sending email without the users knowledge.

The sandbox is managed from a central location to facilitate the distribution of policies to the desktop. The central location will also log events relating to the active content execution. Centralized logging will also assist the IT manager to determine active content use throughout the network.

The whole process of sandboxing the Internet Active Content is intended to be transparent to the desktop user. The only indication to the end user that the sandbox is in place is when some active content activity is blocked. At that point, a message will appear informing the user as to what action was blocked, what program was attempting the action and what options, if any the user has at his disposal.

In summary the Sandbox Technology will:

- Track all files received from the Internet whether from email attachments, downloaded by users, transferred by instant messaging programs. Block the download of these files to the company network if warranted by the company policy.

- Sandbox the execution of all downloaded Internet executable files, regardless of when they are executed and apply the access control rules based on their behavior.

- Sandbox documents received from the Internet when they are loaded into the Microsoft Office programs. Apply the company access control policies regarding what actions these documents can take.

- Sandbox Internet Active Content in email clients and Web browsers. Restrict the actions permitted by these Internet applications based on their behavior and subject to company access control policies.

References

1. Armstrong, Illena, "Mobile Code Stakes its Claim", SC Magazine, November 2000 – Cover Story On-Line Article (11/21/00)
   URL: http:/www.scmagazine.com/scmagazine/2000_11/cover/cover.htm

2. "Why Anti-Virus Alone Isn't Enough – Packers (compressors)", Finjan Website (11/21/00)
   URL: http://www.finjan.com/mcrc/overview.cfm

3. "The Solution for Hybris and other Client-Side Attacks", November 20, 2000, Email mail list from Pelican Security Inc. <info@pelicansecurity.com>

4. Pelican Security Inc., "Active-Content Security: Risks and Solutions", 1999 White Paper
   URL: http://www.pelicansecurity.com/img/assets/1029/W10293910dbbf24c42.pdf

5. "Making the Net Safe for e-Business", Pelican SafeTnet Sales Booklet, 2000

6. Vibert, Robert "The Next War" "Most AV strategies defend against known attacks", Info Security Magazine, September 2000, on-line article (11/21/00)
   URL: http://www.infosecuritymag.com/sep2000/logoff.htm

7. Dean, Richard, "Executive Insights on Content Security: Proactively Addressing Potential Liabilities in the New Economy", White Paper (11/21/00)
   URL: http://www.contenttechnologies.com/products/collateral/pdfs/content_security.pdf