FARONICS™

Intelligent Utilities for ABSOLUTE Control

Blacklist Versus Whitelist Software Solutions

WHITE PAPER

Last modified: August, 2005

Faronics
Toll Free Tel: 800-943-6422
Toll Free Fax: 800-943-6488
International Tel: +1 604-637-3333
International Fax: +1 604-637-8188

www.faronics.com

Blacklist-based Software Versus Whitelist-based Software

A Faronics White Paper

Introduction

The problems caused by malware and malicious code in the form of rootkits and Trojans are multiplying and increasing everyday. The response to these pervasive and escalating problems has created a new industry of antivirus and anti-spyware software and solutions.

This white paper discusses blacklist-based software, one of the most common response solutions in the marketplace that focuses on eliminating or handling the growing problem of malware. It also discusses the relatively new and less common approach of whitelist-based software to combat the problem.

History of Malware

The first virus-like program called Hipboot was seen in the 1970s. The first virus in the wild, seen in 1981, was called Elk Cloner, and was propagated via Apple II floppy disks. Later on, in 1986, two brothers from Pakistan infected the boot sector of a floppy disk with a virus called Brain.[1] This is generally known as the first computer virus in history. That same year, the first PC-based trojan was released in the form of the popular shareware program PC-Write. Some reports say Virdem, often called the first file virus, was also found that year. [2]

In 1990, The European Institute for Computer Antivirus Research (EICAR) was founded in Hamburg in response to the growing number of viruses that were continuing to appear. EICAR released the EICAR test file that is still being used today to validate the correct function and installation of antivirus software on a PC. By the end of 1990 there were over 200 viruses in the wild and dozens of antivirus products on the market to combat the problem.[3] Today, there are an estimated 100,000 viruses in existence, with new ones coming out every day. In addition, there are several new types of malware, including Trojans, worms, adware, spyware, and rootkits, to name a few.

Effects of Malware

Malware can have a serious effect on an organization's technical workspace. It can cause countless hours of downtime while computers are being rebuilt or re-imaged, which takes up a significant amount of infrastructure resources to simply maintain and manage networks. The cost of repairing, maintaining, and preventing malware is growing substantially every year.

Research firm Computer Economics calculates that viruses and worms cost $12.5 billion worldwide in 2003.[4] The U.S. Department of Commerce's National Institute of Standards and Technology says software flaws each year cost the U.S. economy $59.6 billion, including the cost of attacks on flawed code.[5] The FBI rates cyber crime as being its third-highest priority, after terrorism and counterintelligence, but will spend just $150 million of its $5 billion fiscal 2005 budget on it.[6]

As a result of the growing number of attacks, downtime is up. The number of companies worldwide that report downtime of four to eight hours increased from 18% to 22% year over year; those experiencing eight to 24 hours of downtime rose from 18% to 22%; companies whose systems were down for one to three days increased from 7% to 16%.[7]

The increase in hacker intelligence has also led to the serious issue of identity theft. As just one example, in the area of post-secondary education, the Chronicle of Higher Education has reported security breaches on more than two dozen university servers during the last six months, resulting in the compromise of thousands of records of personal data.[8]

Another concern is the problem of day-zero virus attacks, against which there is currently no guaranteed defense. Day-zero vulnerabilities provide a back door into any operating system and represent a serious threat to organizations. InfoSecurity magazine has reported 10 serious day-zero Windows vulnerabilities in late 2004 alone, all of which were exploited by malicious hackers.[9]

It is no surprise that solutions to combat these multiple threats continue to evolve every day.

Solution Overview

One of the largest categories of traditional responses to malware are blacklist solutions, including traditional blacklist solutions such as antivirus and anti-spyware software, and advanced blacklist solutions such as heuristic additions.

Traditional Blacklist Solutions

A blacklist is a list of a particular entity, whether domain names, email addresses, or viruses, that are considered dangerous or damage causing, and are denied entry to the infrastructure they are trying to penetrate. For example, a web site can be placed on a blacklist because it is known to be fraudulent, or because it exploits browser vulnerabilities to send spyware or other unwanted software to a user.

Common examples of traditional blacklist solutions are antivirus and anti-spyware software. Blacklist software works by blocking known threats. Antivirus software companies have a list of known viruses that they provide to their subscribers. When a new virus becomes known, the antivirus companies create a defense against it and provide that update to their users.

Blacklist software can also be used to prevent email spam. Users can create a rule in a spam filter program that prevents email from a particular destination (or matching other specified criteria) from being delivered, even though the spam filter program would have ordinarily allowed it.

Blacklist solution benefits:

- updates to virus lists are automatic and do not require time consuming maintenance
- allows malware to be identified and eliminated
- updates can be done on the fly by an update services server
- offers complete security and protection against all currently known threats

Blacklist solution drawbacks:

- users are essentially giving control of their networks to a third-party vendor, and need to continually update virus and spyware definitions, which increases the load on hardware and network bandwidth
- the modular design is expensive, and difficult to set up and maintain
- the solution requires viruses or spyware to be identified and added to the blacklist, leaving workstations and networks vulnerable to a day-zero attack
- the scanning of all incoming and outgoing IP traffic results in slower workstations
- remote users must obey strict rules to update all definition files on a regular basis to ensure security

---

Bob the Bouncer and Blacklist Technology

Bob is a bouncer at the Hi-Tek Bar. Every night, when the bar opens for business, it is Bob's responsibility to determine who is let in and who is kept out. His supervisors provide him with a list of people who are not allowed in the bar. When these people present themselves at the door, wanting to be let in, Bob finds them on the list and prevents them from entering the bar.

However, if a person on the list shaves his head and grows a handlebar mustache, the next time he presents himself at the bar, Bob may not recognize him and may let him in, where he can do whatever he likes. Additionally, just because someone is not on the list does not mean they are not a threat to the environment, but Bob has no way to know if they are.

Faronics

Advanced Blacklist Solutions

An example of an advanced blacklist solution is heuristic software.

Heuristics is the application of experience-derived knowledge to a problem. It is sometimes used to describe software that screens and filters out messages likely to contain a computer virus or other malware. Heuristic software looks for known sources, commonly-used text phrases, and transmission or content patterns that company history has shown to be associated with email containing viruses. Heuristics is a term coined by antivirus researchers to describe an antivirus program that detects viruses by analyzing the program's structure, its behavior, and other attributes, instead of looking for signatures.

Heuristic solution benefits:

- do not need definition file updates
- may potentially intercept day-zero attacks
- provide another layer of protection because they do not rely completely on definition files
- can sometimes find a threat not listed in a blacklist

Heuristic solution drawbacks:

- makes assumptions about the problem it is trying to solve, and can yield less than optimum results
- legitimate emails in large volume of mail may also fall into the pattern, resulting in many "false positives" and delaying the delivery of valid email
- technology is relatively new; time will be needed to develop and improve it

---

Bob the Bouncer and Heuristic Solutions

Back at the Hi-Tek Bar, Bob's supervisors have decided to try a different approach. Instead of having a list with specific names of people who are not allowed in the bar, they are using a more general set of rules to determine who is and is not allowed to come in. They have based these rules on the kind of people who have caused trouble in the past.

For example, Bob has been instructed to block all people with shaved heads and handlebar mustaches, because in the past, people who have looked like this have caused trouble.

However, unbeknownst to the owner, his son is home from a year of backpacking in Asia with a shaved head and a handlebar mustache. Bob takes one look at him and refuses to let him in the bar because his appearance spells trouble, despite the son being a viable and trustworthy patron.

Faronics

A Different Approach: The Whitelist Solution

Whitelist technology is the opposite of blacklist technology; the list of entities, whether domain names, email addresses, or executables, is a list of what is allowed to penetrate a system. For example, a whitelist of domain names is a list of URLs that are authorized to display, despite any rules of an email spam blocker program.

The most common examples of whitelist solutions are email based, with users creating a list of authorized addresses that they can receive mail from, again despite the rules of an anti-spam program.

Whitelist solution benefits:

- no virus or spyware definition updates are needed; therefore, systems are always protected from day-zero virus attacks
- constant scanning of incoming and outgoing IP traffic is not necessary; therefore, there is no decrease in performance
- no unauthorized executable files, such as a chat program, P2P, spyware, or trojans will ever install or run; therefore, staff productivity increases and downtime decreases
- no illegal or unlicensed software will ever be installed on system workstations; therefore, your organization is not at risk for fines from the Business Software Alliance
- hardware and support budget costs are reduced from a decrease in re-imaging PC's on a regular basis; therefore, organizations can rechannel resources to other activities

> *Bob the Bouncer and Whitelist Technology*
>
> Bob the bouncer, still working at the Hi-Tek Bar, is now trying a third tactic to keep undesirables out of the bar. This time, his supervisors have decided to give Bob a list of people who are allowed into the bar. They are no longer concerning themselves with who is not allowed in.
>
> Bob pays no attention to who might look like a troublemaker based on a general set of rules. He simply lets people who are on the list into the bar. He is a much happier employee now.

Faronics Anti-Executable

Faronics Anti-Executable software takes a different approach to dealing with malware, and it is effective where other software is not because Faronics has designed it to approach security as a system control issue. Anti-Executable allows administrators to choose which applications will be authorized to run on a workstation. Any executable not authorized by Anti-Executable will never install or run. Anti-Executable is based on a whitelist concept, so instead of being configured to block executables that are not wanted on a system, it is configured to authorize executables that are wanted on a system.

In most professional environments, the executables installed on the standard system configuration are the most commonly used programs and applications. There is little need to perform daily dynamic new installations of new programs or applications. Anti-Executable provides a way to ensure all programs and applications loaded as part of a standard system configuration are the only ones authorized to execute. However, adding new executables to the configuration is simple and fast.

Anti-Executable prevents the execution of unauthorized keyloggers, which are the chief tool used in identity theft, and provides protection against day-zero attacks simply because the program will not recognize it as authorized. Downtime as a result of malware is greatly decreased.

Whitelists are a simple and secure option for total system control. The whitelist concept applied to workstation security places all the control in the administrator's hands.

Sources Used

1. http://www.cknow.com/vtutor/IntroductiontoViruses.html
2. http://yahoo.businessweek.com/magazine/content/05_22/b3935001_mz001.htm
3. http://www.infosecurity-magazine.com/comment/050613_eeye.htm
4. http://news.com.com/University+of+Colorado+servers+hacked/2110-7349_3-5800712.html?tag=nefd.hed

Contact Us

Web: www.faronics.com
Email: sales@faronics.com
Phone: 800-943-6422 or 604-637-3333
Fax: 800-943-6488 or 604-637-8188
Hours: 7:00am to 5:00pm (Pacific Time)

Address: *Faronics Technologies USA Inc.*
Suite 170 – 2411 Old Crow Canyon Road
San Ramon, CA 94583
USA

Faronics Corporation
620 - 609 Granville St.
Vancouver, BC V7Y 1G5
Canada

About Faronics

Faronics Corporation develops and markets intelligent utilities for absolute control of multi-user computing environments. Faronics' market-leading solutions have dramatically impacted the day-to-day lives of thousands of information technology professionals and computing lab managers, ensuring 100% availability of systems, thus significantly reducing workstation maintenance, and increasing user satisfaction.

As a customer-centric organization, Faronics' products are researched and developed in close consultation with our end-users. We value our customer's ideas and suggestions, and depend on this feedback to provide the innovative solutions our users have come to rely on. This approach is the basis for Faronics' industry-leading customer service strategy, continually working to build and maintain lasting relationships with our users.

Copyright