Blacklist-based Software versus Whitelist-based Software

Whitepaper

Simplifying Computer Management eurosales@faronics.com www.faronics.com

Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067
Faronics EMEA · Registered in England and Wales No. 6923261 · Registered Office: 130 Wood Street, London EC2V 6DL

Introduction

The risk caused by malware in the form of rootkits, viruses, and Trojans is increasing daily. According to a recent report, threats are increasing exponentially with an average of 73,000 unique pieces of malware detected daily in the first quarter of 2011 . This represents a 26% increase in malware creation rates compared to the same period in 2010.

In response to the explosive malware growth, organizations are demanding more robust security solutions that frequently include two opposing approaches: blacklisting and whitelisting. This white paper discusses blacklist-based software, one of the most common solutions that focuses on handling increasing malware threats. It also discusses the relatively new and less common approach of whitelist-based software to combat the problem.

Malware Motives

Since the first PC computer virus was detected in 1986, malware rates have exploded over the past 25 years. What began as a hobby for technology geeks who were looking for a challenge and seeking fame has evolved into an essential tool for organized crime rings. Today's cyber criminals are professionals who are motivated by the financial benefits of stealing and selling proprietary data, financial records, employee files, medical records, customer lists, and more.

The tools are easy to obtain with malware kits readily available over the Internet. Now even non-technical individuals can become hackers in minutes setting up Trojans and illegal businesses. Hacking is becoming a profession that pays so well that criminals are now investing in their attacks with research, programmers, and testers to stay one step ahead of IT security.

Today, the web is riddled with risk. 90% of breaches were the result of organized crime targeting corporate information. Virtually all of the breaches in 2009 involved customized malware that successfully exposed 140 million records . Given the rising state of breaches, organizations are tightening their IT security infrastructure.

Effects of Malware

Malware is becoming more malicious, detrimental, and costly than ever before. Recent reports indicate an alarming increase in the costs of malware and data breaches.

Cost of Data Breaches

Some estimates say that the cost of cyber crime to the US economy totals mere millions, however others have estimated it at hundreds of billions. A 2010 study conducted by the Ponemon Institute estimated that the median annual cost of cyber crime to an individual victim organization ranges from $1 million to $52 million with the average hovering around $7.2 million, which demonstrates a 7% increase over 2009.

Cost of Identity Theft

According to a 2011 publication released by Javelin Strategy and Research, the annual cost of identity theft is $37 billion, which includes all forms of identity theft, not just cyber means. According to an article published in January 2011, 11.1 million adults from the US were victims of identity theft, which represents a 12% increase over 2008. US fraud totaled $31 billion and across the world, businesses lose $221 billion annually due to identity theft.

Cost of Zero-Day Attacks

Another concern is the problem of zero-day virus attacks, against which there is currently no guaranteed defense. The vulnerabilities exploited by zero-day attacks provide a back door into any operating system and represent a serious threat to organizations. According to the latest research, mutating malware is on the rise as attackers become

increasingly sophisticated. On average, only 15 systems are impacted by a particular piece of malware before it changes to avoid detection and continue to wreak havoc.

Healthcare and education are the two sectors responsible for the majority of data breaches, while financial and government sectors are responsible for the greatest number of exposed identities. The recent headlines indicated that no industry is invincible as even some of the corporate giants and leaders in security have fallen victim to attacks.

Solution Overview

One of the largest categories of traditional response to malware is blacklisting technology, which includes traditional blacklist solutions such as antivirus and anti-spyware software.

Traditional Blacklisting Solutions

A blacklist is a list of specific entities, whether domain names, email addresses or viruses, that contains items presumed dangerous or damage causing, and are therefore denied entry to the infrastructure they are trying to penetrate. For example, a website 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.

The concept of blacklisting 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.

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

Blacklist solution benefits:

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

Blacklist solution drawbacks:

- It only protects against known threats, which often means that someone fell victim to the new threat in order for it to be identified first
- Malware infects an average of 15 systems before mutating and changing it's signature, rendering it undetectable to blacklisting solutions
- On average, antivirus solutions only stop about 19% of threats
- The solution requires viruses or spyware to be identified and added to the blacklist, leaving workstations and networks vulnerable to a zero-day attack
- 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
- Because of its very nature, it is very resource intensive rendering computers slow

Joe the VIP Guest List Manager and Blacklist Technology

Joe is the VIP Guest List Manager at the Hi-Tek Bar. Every night, when the bar opens for business, it is Joe's responsibility to determine who to let in and who to keep out. To help Joe with this process, his supervisors provide a list of people who are not allowed in the bar. When these individuals arrive at the door hoping to be let in, Joe scans the list, finds a match, and denies them entry to 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, Joe might not recognize him. In this, Joe would most likely let him in where he is able to do

whatever he likes. Additionally, just because someone is not already on the "Do Not Allow" list it does not mean that he or she does not pose a threat to the bar. It simply means the bar has not yet caught this individual demonstrating unwanted behaviour, but Joe has no way to know who might be dangerous.

Advanced Blacklist Solutions

Blacklisting solutions have evolved beyond simply banning known threats to include heuristics. Heuristics is the practice of applying experience-based knowledge to solve a problem. In conjunction with antivirus software, it is sometimes used to describe the ability to screen and filter out files that are 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 history has proven to be associated with files 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 simply looking for signatures.

Heuristic solution benefits:

- do not need definition file updates
- may potentially intercept zero-day 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 files in may also fall into the pattern, resulting in many "false positives" and delaying the delivery of valid files or emails
- technology is relatively new; time will be needed to develop and improve it

Joe the VIP Guest List Manager and Heuristic Solutions

Back at the Hi-Tek Bar, Joe's supervisors have decided to try a different approach. Instead of producing a list with specific names and photos of individuals 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 enter. To create these rules, they based them on the types of people who have caused trouble in the past. For example, Joe has been instructed to deny all people with shaved heads and handlebar mustaches because in the past, people who have looked like this have caused trouble.

However, much to the owner of the Hi-Tek bar's surprise, his son has just returned from a year of backpacking in Asia with a shaved head and a handlebar mustache. Joe takes one look at him and refuses to allow him entry because his appearance fits the profile for troublemakers, even though the owner's son is a very good-natured trustworthy patron.

A Different Approach: The Whitelist Solution

Whitelisting technology is the opposite of blacklist technology; the list of entities, whether domain names, email addresses, or executable files, is a list of only 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 familiar example of a whitelist solution is email-based where users create a list of authorized email addresses from which they approve receiving messages, again despite the rules of an anti-spam program.

One of the most important areas of whitelisting is application whitelisting. With application whitelisting only pre-approved programs are allowed to run on a machine and all other programs that are not given the approval status are simply not allowed to run.

Application whitelisting solution benefits:

- provides protection against malware, zero-day, and targeted attacks since no unauthorized executable files can run
- improves employee productivity and workstation processing efficiency because no undesirable applications like chat programs, P2P, spyware, or trojans will install or run
- eliminates the risk of costly audits and fines for license non-compliance since no illegal or unlicensed software will be installed
- saves the organization money by reducing downtime, extending PC lifecycles, and reducing the volume of support tickets creating opportunities for cost transfer to help organizations do more with less

Whitelist solution drawbacks:

- setting up the whitelist can be time consuming unless an advanced application whitelisting solution is used
- managing updates without advanced controls can pose challenges as the updates may slightly alter the approved application's identity from what was already approved on the existing whitelist causing the program not to run

Joe the VIP Guest List Manager and Whitelist Technology

Joe the VIP Guest List Manager is still working at the Hi-Tek Bar. He's now trying a new and third approach to keep undesirables out of the bar. This time, his supervisors have decided to give Joe a list of people who are allowed into the bar. They are no longer concerning themselves with who is not allowed in.

Joe 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 "Approved List" into the bar. He makes no mistakes now and he does not have to worry about getting it right. He is much happier.

Faronics Anti-Executable

Faronics Anti-Executable software takes a different approach to dealing with malware. Anti-Executable allows administrators to choose which applications are authorized to run on a workstation. Any executable not authorized by Anti-Executable will never install or run. Anti- Executable is based on the 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.

The power of application whitelisting has been recognized in the IT community for quite some time. However, the difficulties associated with creating the initial whitelist and the overhead of maintaining the whitelist have prevented many organizations from adopting this security strategy. By harnessing advanced functionality, Faronics Anti- Executable provides organizations with the benefits of application whitelisting without increasing the workload for the IT Team.

In terms of security, Anti-Executable fills the void that antivirus solutions alone cannot. With the tens of thousands of new malware emerging daily, antivirus programs simply cannot keep up with the shocking rates of creation. Given the threats posed by mutating malware, targeted attacks and zero-day threats, relying on catching known threats is no longer sufficient. Knowing that it takes an average of 11.6 days for an anti-virus program to catch a new threat , this leaves organizational networks exposed to serious risk for far too long.

Anti-Executable prevents the two chief tools used in an attack to give control to the hackers. It protects against the execution of unauthorized keyloggers and remote control access programs, which open organizational networks to the criminals. Anti-Executable is the ultimate protection against zero-day attacks simply because the software will not recognize these malicious executable programs as authorized applications. As a result, downtime due to malware is significantly decreased.

Faronics Anti-Executable offers advanced whitelisting technology to help IT Professionals minimize the challenges posed by traditional whitelisting solutions. Including an option to set-up the whitelist upon deployment that alleviates the need for IT staff to manually create a new whitelist for each machine.

Venture House, 2 Arlington Square, Downshire Way, Bracknell, RG12 1WA, England **Tel:** +44 (0) 1344 741057 · **Fax:** +44 (0) 1344 741067

Additionally, the ability to assign trusted publisher status to software manufactures like Microsoft, helps IT professionals to better manage their updates ensuring continuous availability of machines.
Whitelist solutions are a simple and secure option for total system control. The whitelisting concept applied to workstation security places all control in the administrator's hands for even greater peace of mind.

About Faronics

With a well-established record of helping businesses manage, simplify, and secure their IT infrastructure, Faronics makes it possible to do more with less by maximizing the value of existing technology. Our solutions deliver total workstation reliability, complete system control, and non-disruptive computer energy management. Incorporated in 1996, Faronics has offices in the USA, Canada, and the UK, as well as a global network of channel partners. Our solutions are deployed in over 150 countries worldwide, and are helping more than 30,000 customers.

Copyright