

GFI White Paper

Why one virus engine is not enough

Multiple virus engines are needed to reduce time lag between virus outbreak and signature update

There is no single antivirus engine on the market that is always the fastest and most effective at identifying viruses, trojans and other threats. This white paper examines why having multiple antivirus scanners at mail server level substantially reduces the chance of virus infection and explores ways in which this can be achieved.

Contents

| | |
|---|---|
| Introduction..... | 3 |
| The need to have a fast response time..... | 3 |
| Case study: Response to the Worm/Sober virus..... | 4 |
| The need for blending technologies..... | 4 |
| The case for multiple antivirus engines..... | 5 |
| A new paradigm and strategy..... | 6 |
| About GFI®..... | 6 |

Introduction

It is a well-known fact that viruses, trojan horses, worms, spam and other forms of malware present a real threat to all modern-day organizations and affect productivity and business operations negatively. According to the 2008 FBI Crime and Security Survey, 97% of organizations have an antivirus software installed, yet 50% have been affected by a virus attack at least once during the previous 12 months.

Responsible organizations agree that they need to protect their network from virus attacks by installing an email security product. Yet malicious code is becoming more sophisticated and is advanced everyday as virus writers hone their skills and sharpen their code to stay one-step ahead of virus detection methods, penetrating antivirus and firewall solutions with alarming regularity. The success of these viruses is, to a large part, linked to the flawed logic and inherent weakness of protection strategies that are based on a single scanning engine to assess the threat of incoming files.

This white paper explains why the answer to the question: "Is one antivirus engine enough to protect the internal network from mass-mailing viruses, worms and other email-borne threats?" is an emphatic "NO!" It also examines the need for multiple antivirus engines to reduce the average response time to a virus outbreak and thus reduce the chance of having your network infected. The use of multiple virus engines also enables security administrators to be vendor-independent when it comes to virus scanning, thereby able to use the best of breed virus engines available on the market.

The need to have a fast response time

One of the most important factors in the successful protection of your network against viruses is how fast you get new virus engine signature files – those files released by antivirus labs that help to identify a virus when there is a virus outbreak. Email allows viruses to be spread at lightning speed in a matter of hours; and a single email virus is enough to infect your whole network. Obviously then, a critical factor is how fast the signature files of your antivirus solution are updated when a new virus emerges. In every virus attack there is a time differential between the outbreak of the new virus and the release of signatures to defeat and eliminate it. The faster a signature file is created, the less likely the chance of an infection.

Every antivirus vendor in the market claims to have a fast response time. However the reality is not quite so sanguine. Antivirus labs produce updates for virus and worm outbreaks at different intervals. For example, the same lab may produce an update for one virus within six hours, yet take 18 hours for the next one. Complicating the matter further is that while, on average, some companies perform better than others, there is no one company that will always be the first and fastest to respond to a virus outbreak. Granted some companies may be faster on more occasions, but it is never the same company that delivers protection the first. One time it is Kaspersky, the next it is McAfee, another time BitDefender or Norman and so on.

Time differences may also occur that are not the result of the quality of the work or the competency of the lab, but reflect their geographic location and time zone related factors.

Case study: Response to the Worm/Sober virus

The tables below illustrate the response time of antivirus companies to two separate threats.

Table 1 – Response times of antivirus companies to the outbreak of w32.Sober.C

| Company | Time to respond in hours (closest half hour) |
|------------------|--|
| BitDefender | 10.5 |
| Kaspersky | 12.0 |
| F-Prot (Frisk) | 12.5 |
| F-Secure | 13.0 |
| Norman | 15.5 |
| eSafe (Alladin) | 15.5 |
| TrendMicro | 17.0 |
| AVG (Grisoft) | 17.5 |
| AntiVir (H+BEDV) | 19.5 |
| Symantec | 25.0 |
| Avast! (Alwil) | 31.0 |
| Sophos | 35.5 |
| Panda AV | 38.0 |
| McAfee/NAI | 49.0 |
| Ikarus | 56.5 |

Range: 10.5 hours - 56.5 hours, Median: 17.5 hours, Mean: 24.53h

Data taken from the February 2004 VirusBTN issue

Table 2 – Response times of antivirus companies to the outbreak of w32.Sober.Y

| Company | Time to respond in hours (closest half hour) |
|-------------|--|
| AntiVir | 11.5 |
| McAfee/NAI | 40.5 |
| Kaspersky | 43.0 |
| Norman | 60.0 |
| BitDefender | 114.5 |
| Symantec | 116.0 |
| ClamAV | 164.5 |
| TrendMicro | 168.0 |
| Panda | 168.0 |
| Sophos | 170.0 |

Range: 11.5 hours – 170.0 hours, Median: 115.75 hours, Mean: 105.6

Data taken from av-Test.de for November 2005

Clearly, the differences range from hours to even days – more than enough time for your network to get infected!

The need for blending technologies

Every virus lab and scan engine is different. When it comes to protection there is no single best engine, each has its own strengths and weaknesses. Antivirus products often use a mix of technologies to detect and defeat viruses. The three most common approaches are:

Why one virus engine is not enough

- » **Signature files** which are prepared and released by antivirus labs on a regular basis and contain details that help identify a virus. Signature files are the usual way antivirus engines are updated.
- » **Heuristics** are used to detect viruses and other threats that have not yet had signature files developed for them. Essentially they look at different characteristics of a file, assess the characteristics and flag those that appear to be viruses. This method can also detect and catch metamorphic viruses (viruses that can mutate) which are notoriously resistant to signature files.
- » **Sandboxing** isolates and executes suspicious code in a virtual machine isolated from the rest of the IT infrastructure to determine if it's malicious or not.

Individually each of these technologies can be very effective, but it is hard for them to be 100% successful. While some antivirus products combine two or more of these technologies, there is no single best solution. The only effective way to assure the highest level of safety and security is by a multi-layered in-depth defense which can be achieved by using multiple antivirus engines.

The case for multiple antivirus engines

PC SecurityShield estimates that over 40 new viruses are found every day. A 2010 survey by Bit9, "What's running on your users' desktops" found that 68% of IT professionals said they have software restrictions in place, but 45% said they will find unauthorized software on more than half of their PCs.

The argument in favor of using multiple antivirus engines is simple and is predicated on the simple reality that there is no single antivirus engine that does everything. There is no single antivirus engine that is fastest, most effective and "the best" all the time. If you have an engine with the fastest average response time then that is all you have. It does not mean it will be the fastest for the next virus outbreak. It does not mean much if that engine was not the fastest for that particular virus or was not equipped with the right mix of technologies and heuristics; what matters is that your network was infected that one time – with potentially disastrous consequences. The results of the infection and effective "crash" of the system can include lost productivity, lost business, downtime and increased business costs.

Furthermore, from time to time, erroneous antivirus engine updates might seep through since antivirus vendors are constantly trying to release updates as quickly as possible to combat an outbreak. Relying on one single antivirus engine will fail in such an event as viruses might bypass the erroneous single antivirus protection, whilst multiple antivirus engines will provide a backup.

A small caution

While using multiple antivirus engines is a superior solution, it is important to remember precisely what you are getting. Having five antivirus engines does not provide you with five times the protection. It provides you with five opportunities to have the correct answer, each of which are, statistically speaking, independent events. It can be thought of as passing through five security check-in points at an airport where each security check is more or less the same, though each does something slightly different and thus increases your chances of catching a negative event before it happens.

Constant attacks attrite defenses

The previously cited 2008 FBI/CSI study reported that 50% had been affected by a virus attack at least once in the immediately preceding 12 months costing US organizations millions of dollars. Yet the majority of the respondents were users of industry-recognized antivirus software. The failure to protect could almost certainly be tracked back to reliance on a single antivirus engine.

Multiple layers are used in all other forms of security

It is unlikely that you will find an organization that relies on a single security guard or alarm system to protect its most valuable physical assets from a variety of different threats such as theft, vandalism, fire and natural disaster. Instead, there is a multi-layered defense that might consist of security guards, surveillance cameras, sprinkler systems and vaults – all of which have backup systems in the event of failure.

An organization's data, the most valuable asset of all, requires the same multi-faceted defense system and that can only be provided by multiple antivirus engines. You cannot afford to trust any other method.

A new paradigm and strategy

Since it is obvious that single scanning engine defenses are insufficient for the protection of your network then logic dictates a different strategy. Organizations need to implement a layered scanning solution that combines multiple engines to greatly increase chances of having at least one of those virus engines updated on time. Multiple virus engines might also result in the right mix of technological capabilities for any particular threat, thus increasing the chances of your network being protected.

Whilst nothing is perfect, having four or five antivirus engines running simultaneously through a multiple engine manager such as GFI MailSecurity™ for Exchange/SMTP immeasurably increases your chances of getting effective on-time network protection. It also frees you from reliance on the ability of a single vendor to respond promptly and appropriately.

About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

**Disclaimer**

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.