Protecting Against the New Wave of Malware

An Osterman Research White Paper

Published September 2008

SPONSORED BY

Sunbelt Software

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Executive Summary

Managing threats to the endpoint infrastructure is becoming increasingly difficult for most organizations regardless of their size. Viruses, worms, spyware and other forms of malware are becoming more virulent, their authors are becoming more adept at getting around existing defenses, and the profits generated by malware are funding new and more dangerous threats.

At the same time, many anti-virus, anti-spyware and other anti-malware defenses are not keeping up with the growing threats posed by malware. Independent sources have verified that some anti-malware tools are losing ground to the new variants of malware that developers are creating. Adding to the problem is the fact that many administrators view virus remediation and spyware remediation as somewhat compartmentalized offerings that address different problems when, in fact, these problems are actually quite similar in their scope and in the level of threat they pose to endpoints in their organization.

What administrators should consider, therefore, is that malware is malware, regardless of whether the threat is a virus, a worm, a Trojan, spyware code or some other threat. They should also view malware remediation as an integrated set of capabilities that can be managed through a single agent that addresses viruses, spyware, rootkits and other malware in a coordinated fashion.

Malware is malware, regardless of whether the threat is a virus, a worm, a Trojan, spyware code or some other threat.

This white paper, sponsored by Sunbelt Software, addresses the variety of issues facing organizations today in the context of their system management challenges, and discusses the capabilities of VIPRE Enterprise, an integrated platform that provides high-performance, integrated endpoint protection capabilities.

The Current State of Malware

Osterman Research conducted a major study among security-oriented decision makers in the first half of 2008. This study, which was not sponsored by Sunbelt Software, asked these decision makers about a wide range of issues related to the security of their messaging systems, data stores and other parts of the IT infrastructure. As part of this study, Osterman Research asked decision makers to rate the severity of 44 problems on a scale of 1 (no problem at all) to 5 (a very serious problem).

What we found is that viruses and other malware are creating quite serious problems, as shown in the following table. Further, organizations anticipate exposure from a number of problems focused on viruses, malware and other issues, as shown in the next table.

Various Problems Experienced in Managing Messaging and Web Systems
(% Indicating Problem is Serious or Very Serious)

Problem	%
The lag between new virus outbreaks and when our AV vendor issues an update to deal with these outbreaks	25%
Spyware infections	24%
Virus infections	19%

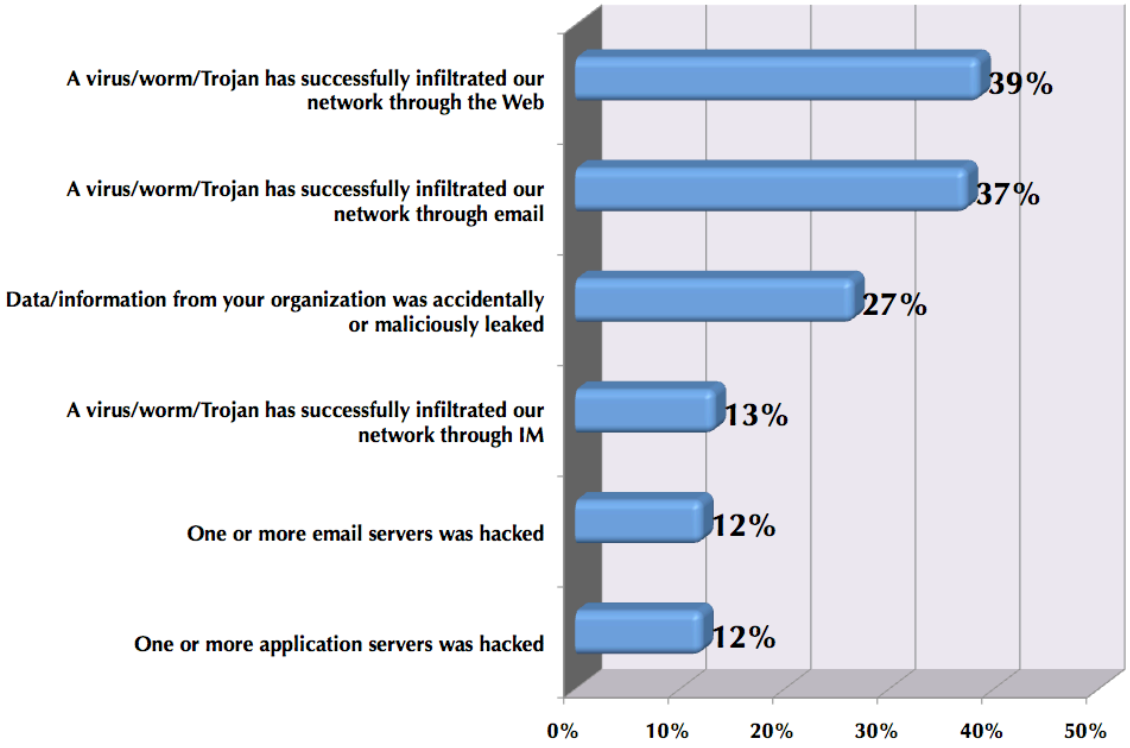
Perceived Risks of Various Security Problems
(% Responding a Serious or Very Serious Risk)

Risk	%
Your users visiting Web sites that could introduce malware into your network	51%
A new virus, worm or Trojan that enters via email harming your network, data, etc.	41%
A new virus, worm or Trojan that enters via a mobile device harming your network, data, etc.	39%
A new virus, worm or Trojan that enters via instant messaging harming your network, data, etc.	29%

THESE PROBLEMS ARE REAL

What this means is that security problems are a serious risk, but decision makers fear that the problems with viruses, worms, Trojans, spyware and other malware will get significantly worse over time. However, these problems are by no means simply anticipated or theoretical: the same survey found that a significant proportion of organizations have already been directly impacted by malware, as shown in the following figure.

Problems That Have Occurred During the Past 12 Months



Clearly, then, these problems are real – they are happening to organizations of all sizes and creating a variety of problems, ranging from annoyance and extra demands on IT staff time to loss of data and revenue. For example, as of August 29, 2008, the SRI Malware Threat Center[1] had detected 29,373 botnet attacks over the previous 456-day period, an average of more than 64 attacks every day.

BLENDED THREATS ARE MAKING THINGS WORSE

Blended threats are payloads that mix several delivery modes (such as email and Web) and often contain multiple components, such as phishing attempts, spam, viruses, worms and Trojans. These threats can combine protocols, such as emails that link to malicious Web sites. This is an increasingly serious threat vector that organizations must consider as they plan their defense strategies.

WHAT YOUR PEERS ARE DOING

The survey noted above found that one in six organizations had switched anti-virus vendors during the 12 months before the survey, indicating that many organizations are not satisfied with the performance of their current anti-virus solutions. Further, the survey found that 69% of organizations will likely or definitely invest in systems to protect against

[1] http://www.cyber-ta.org/releases/malware-analysis/public/

adware and spyware during the next 12 months, and 53% are this likely to invest in systems to protect against zero-hour, email-borne malware threats.

Traditional Anti-Spyware and Anti-Virus Models

Anti-virus software is among the oldest genres of endpoint security. While there is some debate about when anti-virus software was first developed, it is generally accepted that the first PC-based virus was quashed in 1986 or 1987, although the first known virus actually infected ARPANET – the predecessor of today's Internet – back in the 1970s. By 1990, a number of commercial anti-virus products were available from leading developers and the market has exploded since into a multi-billion dollar industry.

A more recent threat has been the emergence of spyware. This is an entire class of malware that covers a variety of threats ranging from simple monitoring of user behavior to provide intelligence for advertisers to intercepting confidential information from infected computers to using those computers for sending malware on command.

> One of the primary reasons that malware authors have been able to defeat traditional defenses is that they are becoming more adept at creating variants of their wares.

The deployment of anti-virus software and, more recently anti-spyware software, on client platforms and servers continues to be a critical best practice given the large and growing number of threats that exist. However, the effectiveness of these capabilities is decreasing over time as malware authors create new and better forms of malware designed to defeat these defenses. For example, a German computer magazine[2] tested 17 different anti-virus scanners and published their results in January 2008. The testers found that effectiveness of these scanners ranged from 20-30%, down from the range of 40-50% that the magazine had discovered in its previous test in early 2007.

WHY ARE TRADITIONAL PRODUCTS LESS EFFECTIVE?

One of the primary reasons that malware authors have been able to defeat traditional defenses is that these developers are becoming more adept at creating variants of their wares. They will create a series of variants of a single threat, each of which has been prepared prior to the introduction of the first variant. Each variant is launched at pre-determined intervals and is able to take advantage of networks' lack of signatures to deal with each new instance of the attack. For example, if each variant were launched at intervals of 12 hours, 100 variants of the same attack would leave open a 50-day window of vulnerability.

[2] c't (http://www.heise.de/ct/)

Another important reason for the decreasing effectiveness of defense capabilities is the use of modular Trojans. Modular Trojans, also known as multi-stage downloaders, operate on a simple principle: a small Trojan first disables local anti-virus software or other security defenses. Once those tools are disabled, a second-stage of the attack downloads any of a variety of threats, including keystroke loggers, worms or other spyware/malware typically designed to take control of the platform. Attackers who successfully disable anti-virus defenses are free to download virtually any sort of malware, including old viruses and other threats, since these will no longer be detected.

The bottom line is that malware is now extremely complex compared to the types of threats that organizations faced just a few years ago. Rootkits, malware that is comprised of several components and the polymorphic variants discussed above make the detection and eradication of malware extraordinarily difficult.

DELIVERY IS BECOMING MORE SOPHISTICATED

Another reason that malware is becoming a more serious threat is that social engineering techniques have become a key infection vector, in many cases using highly sophisticated and creative techniques. For example, some malware developers will display what look like system popups warning of an infection that has been detected or an out-of-date version of software installed on the platform. When well-meaning users click on the "OK" or "Next" button on these fake advertisements, their platform can become infected with malware.

PROFITS ARE UPPING THE ANTE

The fundamental driver for the growth of malware is simple: there are enormous profits to be made from distributing this content, in most cases as widely as possible. While early malware developers and spammers were motivated mostly by notoriety and the challenge of spreading their wares; modern-day attacks are motivated primarily by the prospect of generating huge revenues. Spammers, for example, can earn significant amounts of money by selling products marketed through spam – such as stock "pump-and-dump" schemes – or by directing people to advertising-laden sites on which they earn a commission for clickthroughs.

> The profit motive has dramatically exacerbated the threats from malware. Profits from malicious activities are substantial, they can be used to fund newer and better methods for circumventing defenses.

Malware developers, on the other hand, generate revenue by stealing it. For example, a keystroke logger surreptitiously installed on a client platform can intercept usernames, passwords, bank account numbers, credit card numbers and other sensitive information that can then be used to deplete bank accounts, purchase products or simply be sold to others wishing to do the same.

The profit motive has dramatically exacerbated the threats from malware. Because significant profits are generated by these criminals, many have been attracted to this "market". Further, because profits from malicious activities are substantial, they can be used to fund newer and better methods for circumventing defenses against their attacks. Thus, a vicious circle is created in which malware generates profits that funds better malware that generates more profit.

Next-Generation Technology is Needed

There are a number of good anti-virus and anti-spyware products on the market offered by leading and not-so-leading developers. Some products offer reasonably high detection rates, fairly quick updates of new signatures and minimal impacts on system performance. However, some products do not provide acceptable levels of performance – they are slow to react to newer types of threats, such as the newest types of spyware; some consume enormous system resources; and some are not designed to deal effectively with "grayware" – those applications that typically are more annoying than threatening – such as those that display popup windows or track user behavior.

As a result, the anti-virus and anti-spyware industries are in need of something of an overhaul. For example, while there are discrete anti-virus and anti-spyware products available today, there is no appreciable difference between viruses, Trojans, worms, spyware and other threats from a user's or administrator's perspective. These threats are merely different forms of malware, any of which represent a serious risk to users and organizations alike. It makes sense, therefore, to integrate discrete anti-malware capabilities into a single, integrated platform. An anti-malware system should be designed from the ground up as an integrated set of capabilities that offers:

- A high rate of detection for various types of malware, whether the threat is a virus, Trojan, keystroke logger, adware, etc.
- High-speed detection of threats.
- Minimum imposition on system resources.
- Reasonable pricing for organizations of any size.

About VIPRE Enterprise™

VIPRE Enterprise was built for the administrator that is tired of earlier generation antivirus programs that have bolted on module after module and now are peddling bloatware as a security solution. Instead, VIPRE Enterprise is designed to optimize overall performance by melding anti-virus and spyware protection into a single, powerful engine. This combination of technologies offers high-performance anti-malware software that does not

slow down users' PCs, consumes few system resources, and makes it easy for administrators to protect their networks.

With its next-generation technology, VIPRE Enterprise means powerful virus and spyware protection against today's highly complex malware threats. It eliminates the system slowness and resource headaches of older anti-virus products. The many capabilities of VIPRE Enterprise include:

- **Checkmark Anti-Virus Certified**
  VIPRE is Checkmark Anti-Virus Desktop certified by West Coast Labs and will receive additional certifications through other certifying bodies throughout the balance of 2008 and into 2009.

- **Powerful, comprehensive scanning agent technology**
  VIPRE Enterprise employs a high-speed, threat-scanning engine that can scan large volumes of information for malware threats in a short period of time with limited performance impact on the end user's machine. With its optional agent user interface, users can stop and start scans and manage their own quarantines.

- **Real-time monitoring with Active Protection**
  VIPRE's Active Protection delivers real time monitoring and protection against known and unknown malware threats. Active Protection works inside the Windows kernel, watching for malware and stopping it before it has a chance to execute on a user's system.

- **Configurable dashboard provides a centralized, policy-driven management console**
  VIPRE Enterprise supports multiple methods of agent deployment to allow administrators flexibility in how agents are pushed to their users' systems. Within the Admin Console, an agent deployment wizard helps administrators select a deployment option and assists them with their deployment configuration: silent push install, MSI file, Active Directory Policy based on OU's, IP range and machine lists.

VIPRE Enterprise employs a high-speed, threat-scanning engine that can scan large volumes of information for malware threats in a short period of time with limited performance impact.

- **Policy-based management**
  VIPRE Enterprise has sophisticated policy creation and management functionality that gives administrators the flexibility to control scheduling of quick scans and deep scans, set scan options (including scanning of known locations, whether to scan cookies, and whether to scan running processes), and allow specific threats from the database.

- **Flexible Reporting**
  VIPRE Enterprise's reporting features make it easy for administrators to schedule and

customize its library of reports. A report scheduler allows administrators to easily schedule any report to run at a designated time with the ability to email reports to specified users; simplifying report distribution to management. Additionally, a custom report editor enables administrators to modify existing reports or create their own reports.

- **Resource Usage**
  Old-style anti-virus products have stacked layer upon layer of engines, and created bloatware in the process. VIPRE imposes a low impact on system resources compared to the competition.

Summary

Malware is a serious threat and the problems are getting worse. Authors of malware are becoming more adept at circumventing the billions of dollars in anti-virus, anti-spyware and other endpoint security defenses that have been deployed by organizations of all sizes. Because malware authors are motivated by profit – and successfully generating lots of it – they are able to create ever more sophisticated ways of breaching these defenses.

At the same time, many anti-virus and anti-spyware tools have not kept pace with the threats. They are less effective at detecting the growing array of threat variants, they impose a huge burden on system resources and they are expensive to deploy and maintain. What organizations need, therefore, is a capability that provides high detection and proactive protection against known and unknown types of malware, an integrated approach to dealing with viruses, spyware, rootkits and other threats from malware, and robust management tools that will minimize administrator involvement in the process of manage threat remediation.