

Protection Against Blended E-mail Threats

STOPPING WHAT TRADITIONAL ANTI-VIRUS
PRODUCTS CAN'T

INTRODUCTION

E-mail viruses have evolved from fun hacker experiments for notoriety, to financially-motivated, sophisticated attacks that change constantly to defeat traditional defenses. Recent headlines have shown the devastating results of company data compromised. Fallout from these attacks includes both direct financial consequences as well as loss of customer trust and irreparable damage to the company's image.

Almost every week, technical and business media report on a new worm or virus that exposes corporate or customer data. Because the main mechanism to spread these viruses is e-mail, no company, small or large, is immune to these changing and more sophisticated threats.

To combat these more advanced attacks, Avinti has developed iIsolation Server™ to stop threats such as zero-day threats, targeted attacks and first-instance malware that are not detected by traditional anti-virus products. Available as a product or as a managed service, the iIsolation Server uses a proprietary, high-performance Observation Engine™ that observes malware behavior to proactively and safely block threats before they reach internal mail systems.

NEW HACKER MOTIVATIONS

Over the last decade, virus writing has evolved from hobby to cottage industry to a thriving growth industry. Early virus writers, motivated by technical challenges and the chance for notoriety, developed relatively benign viruses and worms that caused low to moderate damage. These viruses, which often gained significant media attention in the late 1990's and early 2000's, caused damages mainly in the form of clean up costs and productivity losses, but with minimal impact on company and confidential customer data.

However, as with any growth industry, the potential for financial reward has greatly increased the stakes. Today's virus writers are more likely to be motivated by financial gain and use malware to steal company data and confidential customer information. Recent studies have indicated that as much as 69% of malware written today is specifically written to steal confidential information¹. And like any industry, motivations for profit lead to a constant flow of new innovations as hackers look for new sophisticated ways to get past existing security measures.

NEW HACKER TOOLS

- Zero Day Malware Attacks
- Targeted Threats
- Mass Variant Attacks
- Blended Threats

NEW ATTACK VECTORS

New innovations in the malware industry have increasingly focused on avoiding detection by traditional anti-virus products through different tactics. Introducing new viruses, for example, has historically been the simplest way to avoid detection by signature-based anti-virus products. These anti-virus products are reactive, relying on having seen the virus previously and a definition or "signature" of that virus been written in order to detect the virus in the future. The use of such new "zero-day" or first-instance malware has consistently yielded results in avoiding detection before a new virus is found and definition files are updated. The use of new malware to beat existing anti-virus security products continues to rise, with a 39% increase of new viruses detected in the second half of 2006 over the first half of the year².

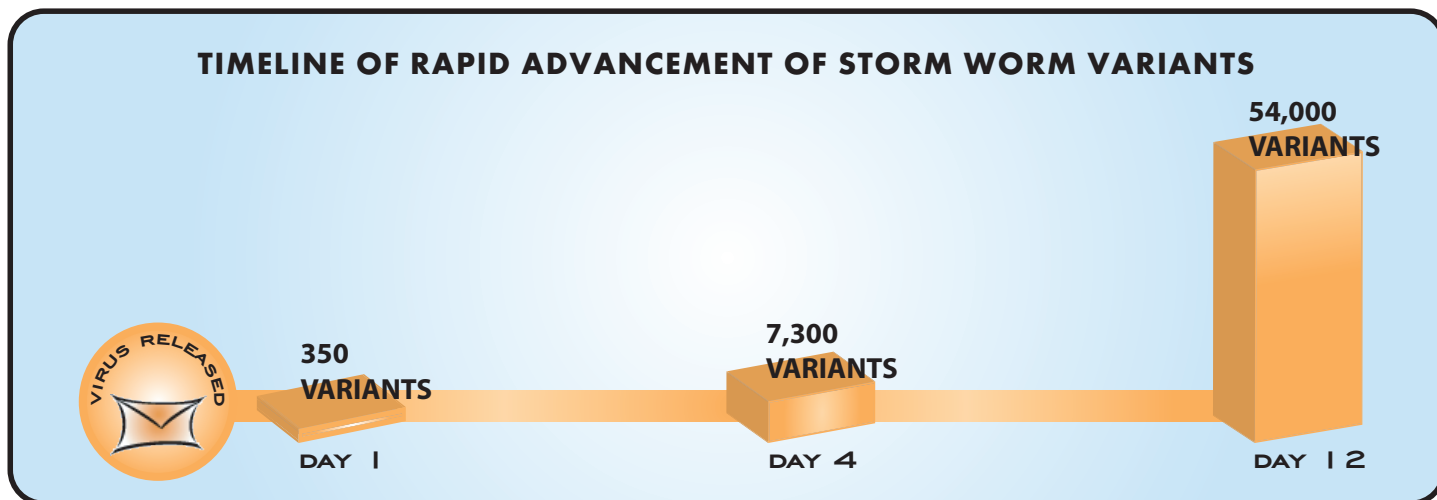
Also, the use of stealthy targeted threats has increased dramatically. These e-mail-based attacks, which are often sent to one or a few individuals, are designed to circumvent signature-based products and IP reputation services that rely on previously-written signatures or high volumes of traffic for detection. Even more threatening, these targeted threats are highly customized and may appear to come from familiar internal or external sources, dramatically increasing their success rate. Very frequently, the threats use common Microsoft Office™ documents such as Word™ or PowerPoint™ to infect the user's system.

In addition, the use of malware variants has been a successful tool of virus writers to avoid detection. Variants of previous malware are easily generated using automated tools that are available to experienced and inexperienced hackers alike, and have proven to be more than a nuisance to virus definition writers.

¹ Symantec Internet Security Threat Report, Trends for July-December 06, p. 13

² Symantec Internet Security Threat Report, Trends for July-December 06, p. 54

While the use of variants has often strained the resources of anti-virus labs to keep up, lately this technique has been taken to new extremes, as evidenced by the Storm Worm launched in January 2007 (see sidebar below). This use of a massive number variants, some of which generate only a small amount of traffic to avoid detection, is in effect a denial of service attack that overwhelms virus signature writers. There doesn't appear to be an end in site for this effective virus writing tool. In fact, a recent report by the Yankee Group entitled "Anti-Virus is Dead" predicts that the number of unique malware variants in 2007 to reach 220,000, a ten-fold increase over 2002, only increasing the difficulty of traditional anti-virus products to keep up with both new malware, and vast numbers of variants³.



The use of malware variants has been a popular tool, but the Storm Worm, which first emerged in January 2007, has taken these attacks to a new level. Engineered to overwhelm traditional signature-based defenses, the first day Storm Worm presented approximately 350 variants that were designed to stay ahead of traditional anti-virus solutions by overwhelming them with a large volume of minutely-different viruses. By the fourth day, approximately 7,300 variants had been launched; and by the 12th day, more than 54,000 variants were waging a assault on networks worldwide. The effect of these attacks was to overwhelm traditional signature-based products and allow large numbers of small-volume variants to slip by anti-virus and reputation based products. It was a shockingly stark example of the ease in which virus writers could overwhelm existing defenses and led the CEO of one anti-virus company to declare, "This is a competition where the anti-virus companies, I fear, are not in a good position."⁴

The nature of these and other new threats designed to avoid detection, have placed traditional anti-virus vendors on a virtual treadmill where they are forced to continuously try to keep up with both the volume and the sophistication of an onslaught of new attacks. This has led some to declare the end of signature-based anti-virus as a viable solution to the problems today's corporations face.

BLENDING THREATS

Increasingly, a new attack vector is being used to lure users to download malware through methods other than e-mail attachments. Hackers using alternative channels to breach corporate IT systems are developing blended threats as a new tool of choice. E-mail blended threats use e-mail as the initial vehicle to launch the attack, without relying on attaching a virus to the e-mail itself. Examples include the use of HTML-based e-mails containing active content such as JavaTM, JavaScriptTM, or ActiveXTM or embedding URLs in the e-mail to link the user to Web sites where malware can be downloaded in the background often without user intervention. These attacks are missed by anti-virus products looking for malware attachments, and which have no ability to view the links and active content in the context of an end user. They are also missed by Web filters that may not block URLs linked to malware or by filters that have not been alerted to or rated a hacker's newly-constructed Web site.

Adding to the threat, these e-mail attacks are well-engineered to trick users into believing that the message and the Web site are legitimate and lead to trusted Web sites. Even more alarming is the increasing use of legitimate Web sites that are hacked for the purpose of infecting them with malware that is downloaded. In a recent incident, the the Miami Dolphin's Web site that was

³ Anti-Virus is Dead; Long Live Anti-Malware, Yankee Group, January 17, 2007
⁴ Stormy Weather for Malware Defenses, Security Focus, March 03, 2007

hacked and infected with malware for over a week. This demonstrates the problem of users going to a trusted Web site that would not be detected by a Web filter. Users may even spread these attacks by unknowingly sending or forwarding e-mail on that contain links to malware inserted into popular Web and social networking sites, known as the “Youtube Syndrome.” Experts agree that attacks on these popular sites will continue, leaving the door open for hackers to spread malware through these high-traffic channels.

Some blended threats do not even require the user to click on links in the e-mail or visit a site. Active content embedded in the e-mail can be activated via the preview panel of the user’s e-mail program.

The extent of the blended threat problem has even reached the attention of the Federal Trade Commission which emphasized their concern for this type of attack in a recent report:

“Another troubling development is an increase in the use of spam that deploys malware on recipients’ computers. This can occur when a recipient clicks on a link in spam that lures the recipient to a Web site where his computer will become infected with spyware or other types of malware. In some instances...merely opening a malicious e-mail can subject the recipient to harm from malware.”⁵

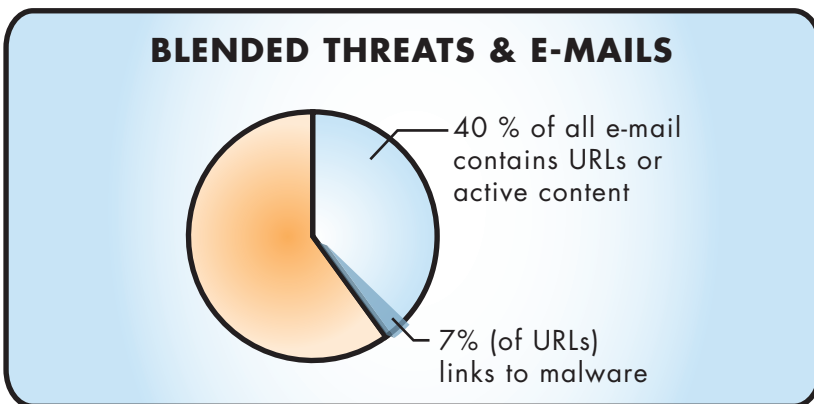
Blended attacks expose users’ systems to hackers who may then access personal or corporate data; incorporate the computer into a network of bots and launch other attacks; log user keystrokes to get passwords and other information; or simply allow the virus to propagate itself.

BLENDING THREAT SUMMARY

Blended threats can:

- Easily slip by anti-virus engines because the malware is not in the body of the e-mail, but downloaded from a Web site or through active content
- Elude most Web filters as they are security related, not content-related
- Run in the e-mail content itself through the preview pane, without any user intervention (in the case of active content).

SIZE OF THE BLENDED THREAT PROBLEM



Avinti’s own research team has found up to 40% of all e-mail contains URL links or active content, of which more than 7% link the user to Web sites where malware is downloaded to the user’s system.

⁵ Federal Trade Commission Report, December 2005

REQUIRED PROTECTION

The nature of the problem of blended threats requires a solution that is designed to see and validate the threat and remove the guesswork involved in associating the e-mail with a Web-based threat.

Validating blended threats requires a new protection strategy that includes the ability to:

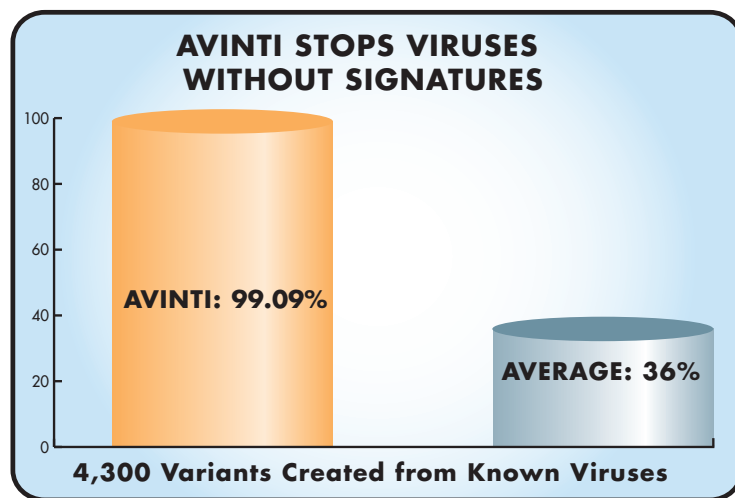
- Review all e-mail components: the e-mail body, attachments, active content, and links in context
- Safely observe the active content and the URL links to the Web
- Review and determine the extent of the threat based on actual behavior.

iSOLATION SERVER™

Avinti's iSolation Server, a proactive security solution, is designed to stop stealthy, complicated threats such as zero-day malware attacks, targeted threats, blended threats, and mass variants. Its patent-pending technology complements existing security solutions by detecting threats without the use of signatures.

Avinti's approach is unique because it safely observes actual behavior of potentially threatening messages, rather than relying on reactive signature-based approaches. iSolation Server first sorts e-mail based on administrative parameters to identify potential threats. Clean messages are delivered immediately to the e-mail server, while high-risk messages are sent to the high-performance Observation Engine™. The Observation Engine proactively observes the actual behavior of the message or content in a secure and protected environment — then quickly delivers clean messages while quarantining malware and other identified threats.

In a recent study conducted by an independent lab, iSolation Server was tested along with seven other anti-virus software vendor solutions using custom created malware variants designed to mimic common avoidance detection techniques. The test included over 4,300 variants that were created from known viruses, using tools similar to those used by malware authors to create new variants. The results showed iSolation Server to be effective at catching 99.09% of all malware variants, compared to an average of 36% for other products tested.⁶



⁶ Avinti iSolation Server Comparative Test Results, Independent Security Evaluators, May 2007

BLENDING THREAT PROTECTION™

Avinti has now extended its unique, patent-pending technology used to detect e-mail-based viruses, including first-instance and targeted threats, to solving the problem of blended threats. iSolation Server now searches the body of the e-mail for active content and URLs. It quickly filters URLs and active content, taking action on known exploits with its déjà vu filtering technology. It then observes the behavior of potential blended threats with the Observation Engine, which observes the active content as well as clicking through to the actual URLs. Multiple instances of the Observation Engine provide the performance to handle large traffic volumes and administrator settings provide options to blacklist and whitelist URLs as well as block, warn, or neutralize the e-mail-based active content. Because Avinti's approach doesn't rely on signatures, it is effective at catching new exploits.

iSolation Server integrates Blended Threat Protection in order to:

- Scan incoming e-mail for blended threats (URLs and active content)
- Evaluate e-mail in context for suspected threats
- Compare content with previously known threats
- Run the active content based e-mail or URL in a virtualized environment to determine if malware is present
- Modify or blocks the offending e-mail to protect the end user.

The changing nature of malware threats requires new, smarter solutions to protect users from attacks. Avinti's iSolation Server is uniquely capable of blocking the advanced threats faced by companies today, including traditional viruses and spam, zero-day malware attacks, targeted threats, and mass variant attacks, without the use of signatures. With the addition of Blended Threat Protection, iSolation Server proactively detects and blocks blended threats before e-mail reaches the user, without relying on a separate Web filter. Through its unique Observation Engine, Avinti's Blended Threat Protection stops even new viruses that would pass by other anti-virus engines.

iISOLATION SERVER TECHNOLOGY & BENEFITS

Technology	Benefits
1) Observation Engine observes e-mail attachments for existing and new viruses	<ul style="list-style-type: none"> • Stops problematic threats: <ul style="list-style-type: none"> • Zero-day malware attacks • Targeted threats • Mass variant attacks
2) Proactively stops blended e-mail threats such as URLs and Active Content	<ul style="list-style-type: none"> • Stops new attack vectors in the e-mail itself • Protects valuable corporate data • Prevents social engineering through targeted attacks • Stops blended threats before they reach end user: <ul style="list-style-type: none"> • Prevents preview pane attacks • Protects remote network and home-based end users
3) Observes actual behavior of threats	<ul style="list-style-type: none"> • Highly accurate catch rate • Very low false positives
4) Uses variable blended threat policy settings	<ul style="list-style-type: none"> • Administrators may block or allow specific URLs or domains • Flexibility to block, warn, or neutralize content • Permits blocking and observation of productivity harming URLs

BENEFITS

Unlike other anti-virus products, Avinti's iSolation Server proactively blocks blended threats and blocks even new attacks and malware without signatures.

Blended Threat Protection benefits include:

- *Preventing blended attacks delivered via e-mail with embedded URLs and active content*
- *Protecting confidential information*
- *Blocking and productivity-reducing URLs through policy settings*
- *Warning, neutralizing, or blocking e-mails through policy settings*
- *Proactive protection that prevents attacks from ever reaching user systems, regardless of network or location*

SUMMARY

As hackers are becoming more sophisticated, the use of new tools such as blended threats to obtain valuable financial and personal information has increased. The use of blended threats that include URLs and active content in e-mail are undetectable by traditional anti-virus products. The addition of Blended Threat Protection to Avinti's iSolation Server makes it uniquely capable of stopping these new threats quickly and effectively, before they reach the end user.