Malware Today and Mail Server Security

Trend Micro Security Solution

Driving the Need for Highly Effective Mail Server Security

Increasingly Sophisticated Threats Elude Traditional Defenses

A Trend Micro White Paper | January 2008

CONTENT

I. YOUR THREAT IS IN THE EMAIL

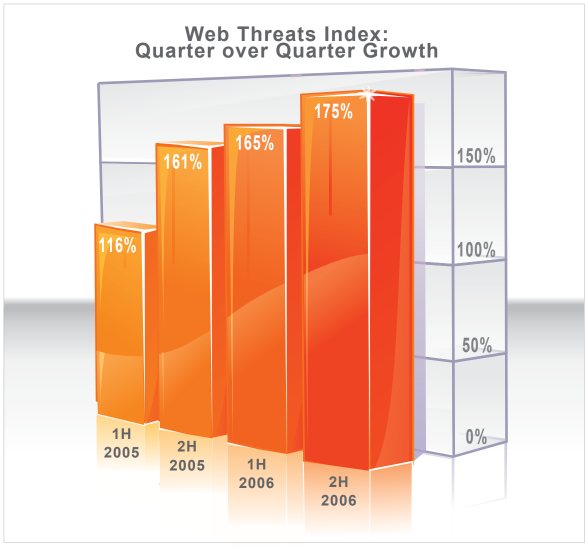
From Chaos to Cash

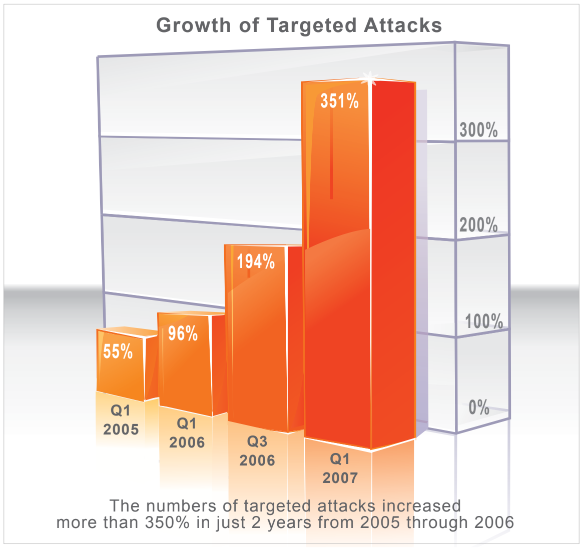
Enterprise security professionals understand that the motivation behind malware has shifted from creating chaos to making money. Cybercriminals reap financial gain by stealing and reselling valuable information: credit card numbers, personal identities, intellectual property. Others propagate Trojans to take control of inadequately protected computers and servers, using them for future malicious endeavors or renting them to others for spam blasts, Denial of Service (DoS) attacks, malware campaigns, or targeted attacks. Trend Micro has documented this shift extensively and many resources, including a 2007 threat roundup, can be found on the Threat Resource Center at http://itw.trendmicro.com.

The Bad Guys: Smarter and More Determined

Most enterprises today have already invested substantially in email security. However, yesterday's defenses may not be up to the challenge of tomorrow's threats. Why? Because cybercriminals today are well-organized, have access to more talented software engineers, understand the strengths and weaknesses of traditional defenses and are highly motivated by the lure of monetary gain. In a word, they're just better than they used to be.

Researchers at Trend Micro's global threat-sensing network, TrendLabsTM, track existing and emerging threats closely—and what they have seen recently is sobering. In particular, the volume and virulence of malware that attacks the enterprise via Web browsing and email is skyrocketing: Web threats are growing more than 100% every six months and targeted attacks are up 351% from two years ago. This continued evolution of threats has spurred enterprise security managers to take a fresh look at their messaging security, especially at the mail server.


Web Threats Index:
Quarter over Quarter Growth


Growth of Targeted Attacks

The numbers of targeted attacks increased more than 350% in just 2 years from 2005 through 2006

II. KNOW YOUR ENEMY

This paper will provide you with practical advice for how you can improve your enterprise's defenses, especially at the mail server. But first, let's take a closer look at a number of threats that are representative of the the latest generation of malware:

- TROJ_PROXY
- NUWAR
- YABE
- STRATION

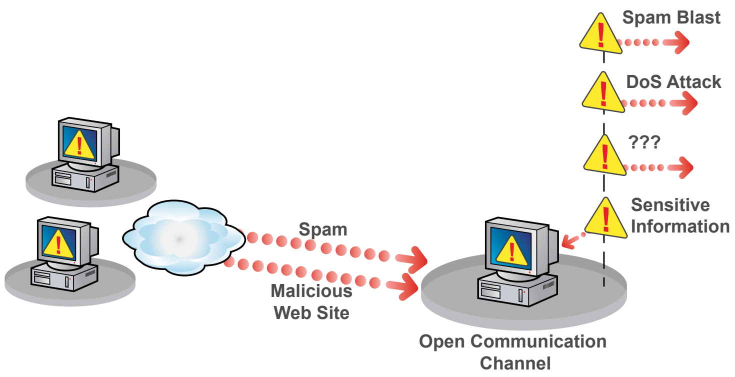
TROJ_PROXY
Threat Targets Both Email and Web Browsing

On June 5, 2007, Trend Micro discovered a new and particularly insidious malware attack: TROJ_PROXY. AFV. This threat is propagated concurrently through downloads from Web sites or as attachments to spammed email. To entice users to open the attachment, the email contains subject lines gleaned from actual news headlines and .ZIP attachments that appear to come from news organizations.

How TROJ_PROXY Works

When a user opens the attachment, TROJ_PROXY registers itself as a system service that executes automatically at system startup. It connects to malicious Web sites to download additional malware or await further instructions. This effectively turns the infected machine into an open proxy server that can be used for the attacker's purposes.

TROJ_PROXY in Action



Defending against TROJ_PROXY

If an organization has vulnerabilities in either its email or Web browsing security, the risk is high that TROJ_PROXY will be successful in infecting machines inside the perimeter. Detection requires:

- Coordinated efforts between both email and Web security experts
- Dedicated spyware protection at the email getway and mail server to stop the latest Web-based threats from entering via email
- Strong anti-spam detection to stop incoming attacks by identifying malware-carrying spam campaigns

Read the complete Trend Micro report on TROJ_PROXY.

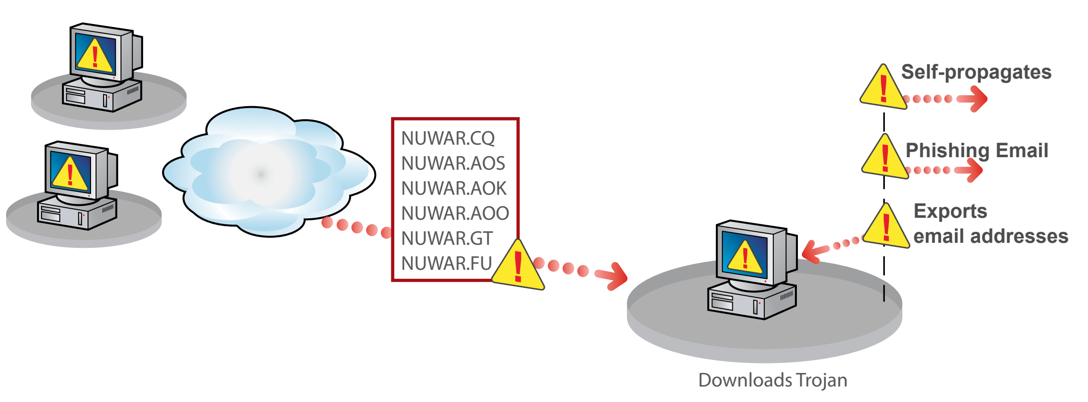
NUWAR
Multiple Components, Multiple Variants Can Overwhelm Inadequate Defenses

NUWAR exemplifies the multicomponent threat, which combines a number of malware techniques. It defies categorization: NUWAR can be accurately called worm, Trojan, rootkit, spyware, and spam. NUWAR uses infected machines to launch spam attacks both for financial gain and also as a mass-delivery mechanism for itself and other malicious code. A particularly profitable use is the so-called “pump and dump” scheme, designed to artificially inflate a penny stock. This type of attack now accounts for as much as 25% of all spam today.

How NUWAR Works

Spam emails sent by NUWAR also carry NUWAR itself, so the number of infected machines can grow geometrically unless effective defenses are in place. Trend Micro detected more than 40 variants of NUWAR in a two-week period in late 2006. These variants present different digital signatures to defeat security programs that rely exclusively on signature-based defenses. In addition, the NUWAR Trojan downloader can also install new variants—in effect, NUWAR contains its own upgrade engine! Still registering among the top 10 threats in October 2007, the latest attacks harvested email addresses from DHTML files on the infected PC to self-propagate to friends and family when the user communicated via Webmail.

NUWAR in Action



Defending against NUWAR

Because of its mixed nature and many variants, the most effective defense against NUWAR includes:

- Signature-independent zero-day threat detection to detect variants
- A strong antivirus scan engine with dedicated spyware protection to prevent Trojan downloaders
- An effective anti-spam engine to stop malicious incoming email and, in the event of an initial infection, to detect internal and outgoing campaigns
- Protection at both the gateway and mail server to combat the heavy use of variants

Read the complete Trend Micro report on NUWAR.

YABE
Regional Password-stealing Attack Uses Compression to Avoid Detection

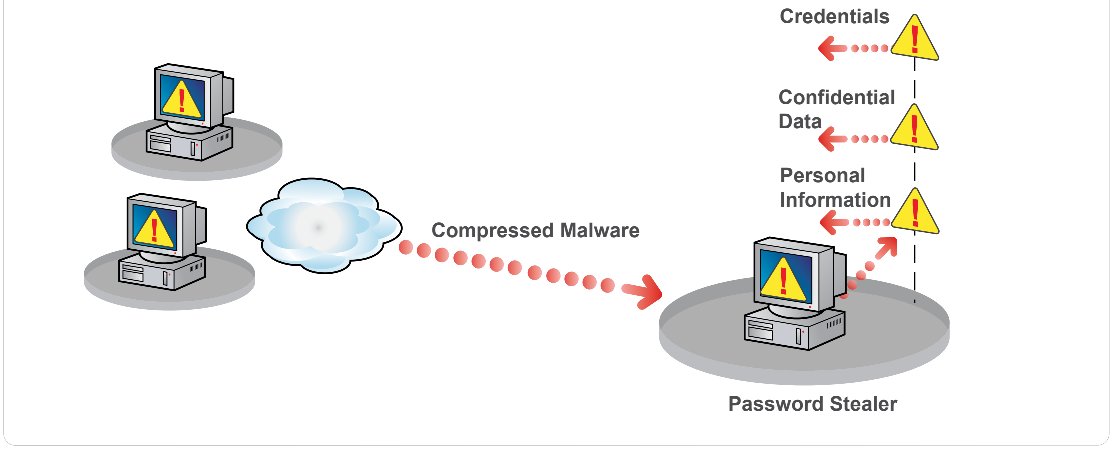
This regional attack—found primarily in German-speaking and Nordic countries—gets its name from its original attempt to steal eBay account information: YABE is eBay spelled backwards. Since then, it has broadened to pose a threat to any personal banking information that can be used for fraud and, increasingly, to portal login credentials of all kinds.

How YABE Works

YABE uses compression tools—common ones are Neolite and PEPack—to avoid traditional email security detection methods in order to reach users. These schemes quickly vary YABE's binary code to avoid pattern file matching.

Once delivered to users, YABE's social engineering gambit takes advantage of the increased trend of online invoicing. An attached Trojan masks itself as an invoice attachment, utilizing the default setting for Windows Explorer to hide its .EXE extension. This legitimate-looking .PDF file name, accompanied by the Adobe Acrobat icon, entices many users to open the file. Once opened, it installs a password stealer that collects login data from online banking sites visited by the unsuspecting user, as well as credentials for Web sites and email clients, sending them on to the cybercriminal.

YABE in Action



Defending against YABE

As with NUWAR, traditional signature-based defenses alone cannot stop YABE. Derailing this threat requires:

- Signature-independent zero-day detection, ideally with the ability to identify the use of non-standard compression tools favored by attackers
- True file type scanning that can look deeply into compressed attachments to flag malicious files

Read the Trend Micro blog about a recent wave of YABE attacks.

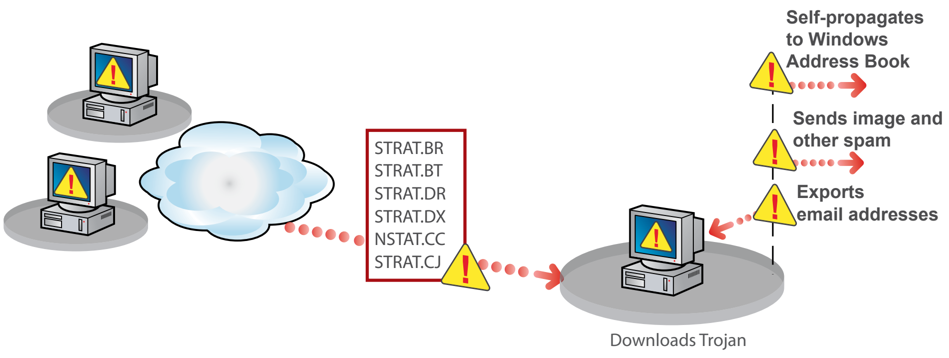
STRATION
Spam Propagates Malware

In September 2006, in the face of increasing infections and seemingly endless releases of new variants into the wild via spam campaigns, the Trend Micro Japan office declared an alert to control the onslaught of WORM_STRATION. This threat quickly gained the notoriety for spawning variants at an alarming rate: Trend Micro documented 155 variants in a single month. Within weeks, WORM_STRATION was also found spreading rapidly in the United States and the rest of the world. Variants of this malware have been seen more than a year later.

How It Works

The social engineering ploy of STRATION is like a criminal disguising himself in a police uniform. The spam email claims that the recipient's computer is infected, and that the attachment will clean it up. In reality, the attached executable is a Trojan downloader that turns the user's machine into a spam zombie. STRATION is unique in the speed at which it spreads. Once infected, the machine downloads and installs a number of executables. It then locates open mail proxies through Domain Name Service (DNS) queries and uses them to send out spam. In addition to the content—often an image file advertising pharmaceutical products—the spam also includes a copy of the Trojan downloader attachment, potentially propagating STRATION to every email recipient. STRATION mines email addresses from the Windows Address Book of the infected PC, so target recipients are often co-workers within the organization.

STRATION in Action



Defending against STRATION

While the malicious code itself is technically a worm, its method of propagation—both to initially penetrate and then propagate within the organization—is through spam. Therefore a complete defense, above and beyond basic antivirus scanning includes:

- Effective spam detection to stop the mass mailer campaigns known to widely disseminate STRATION
- Strong generic detection methods within the antivirus scan engine to detect variants of the malicious attachment within incoming and internal email
- Protection at both the email gateway and mail server is needed to stop the initial infection as well as to prevent internal propagation

Read the full Trend Micro report about STRATION.

III. WHY THE MAIL SERVER MATTERS

The preceding examples show that the new generation of email-borne threats requires significant strengthening of security defenses. However, the specific steps needed vary widely, depending on the security infrastructure already in place.

Email Gateway: Always the First Line of Defense

Much of the recent messaging security investment, primarily driven by the huge volume of spam over the past few years, has been at the email gateway. Since a large number of attacks originate outside of the organization, and every incoming email message enters the enterprise via this gateway, it is a logical place to mount an effective defense. Obviously, the optimal situation is to keep all unwanted and malicious email out of the organization entirely, and the gateway is the place to start. However, with many organizations receiving hundreds of thousands of unwanted or malicious messages (or more) per day, even 99% effectiveness can let high-risk messages through.

Client Security: Vital, but Not Enough by Itself

The ultimate goal of every email-based attack is to infect as many clients as possible. For this and many other reasons, client security is an essential component of a complete enterprise protection system.

However, client security alone cannot do the job. The modern network is accessed by an increasing number of remote and mobile clients. The task of ensuring that every one of these has the latest security software and signatures updates—as well as operating system patches—is daunting. It only takes one noncompliant client to create a gaping hole in network defenses. Even successful detection at the client has cost: Users can be inconvenienced and confused by error messages and flood helpdesk resources with calls.

Mail Server: Critical Link in the Multilayered Defense

No matter how effective the perimeter defense, there is still a need for strong protection at the mail server. While security vendors strive for 100% detection in all their products, including those for email gateway security, there is always a risk of something slipping through the gateway, especially given the use of high volume delivery via spam campaigns and multiple, often serial, malware variants. There is also significant risk of threats entering the network through an out-of-date mobile user. Interestingly, in a recent Trend Micro customer survey (September 2007), 72% of customers cited mail server security as a critical second line of defense for incoming email.

However, since every email-borne threat must reside on the mail server at some point, it provides an ideal second chance to stop incoming attacks. It is also the only central inspection point for internal communications and propagation such as those initiated by STRATION. The need for a strong multilayered defense—with particular emphasis on the mail server—is clear.

IV. CHOOSING THE RIGHT SECURITY VENDOR

In light of the evolving nature of malware attacks today—especially those entering through email—enterprise security professionals are constantly looking for ways to bolster defenses.

Choosing the right vendor is a crucial step. Here are key criteria you need to assess:
- Range of security expertise
- Signature-independent protections in addition to traditional scan engines
- Anti-spam defenses—even though the intention is to stop malware
- Support services

Broad, Deep Security Expertise

As pointed out in the threat section earlier, the new breed of blended threats are difficult even to categorize, let alone defend against. When you choose a security vendor, it is vitally important to consider core expertise—both in the areas of email and Web security. The plain fact is that many—if not most—of the tier 2 and 3 vendors simply don't have the resources and experience to combat a wily foe such as NUWAR or YABE.

When evaluating a security vendor, focus on the company's broad capabilities in research, service, and support. Also be sure that the vendor you choose can support you 24/7 and respond to new threats in real time—an absolute prerequisite for effective defense. Finally, the vendor needs expertise across the full range of threat technologies, including spam, adware, spyware, malware, crimeware, botnets, phishing, and rootkits.

Beyond Signature-based Defenses

Many vendors offer a traditional signature-based malware defense. All these offerings are not equivalent: top-tier vendors who invest heavily in malware signature generation will always have the edge over smaller competitors. And a highly-effective antivirus scan engine is just one element of protection. To combat the elusive techniques of attacks like YABE and NUWAR, other key elements include signature-independent zero-day protection and threat management services to stop new attacks and their variants.

Advanced Spam Detection

Given the use of spam campaigns to not only advertise products or stocks, but also to deliver malware (as seen in 3 of the 4 attacks detailed earlier) a vendor's anti-spam solutions also play an important role in reducing the risk of compromise. Look for vendors whose security products include a range of detection techniques including those that continually expand to quickly address the latest campaigns and techniques.

Top-notch Support, When You Need It

No one wants to go it alone in this complex, high-stakes game of threat defense. When you choose a security vendor, it's important to look not only at the products, but the people behind those products. Ideally, your vendor has the expert human resources needed to back you up—and a way to access them that doesn't involve hours on hold, listening to recorded music.

V. WHY TREND MICRO FOR MICROSOFT EXCHANGE

The security market has recently seen a number of new entrants into email security, including Microsoft™ with its ForeFront™ brand. Unlike many of those new competitors, Trend Micro is a security specialist. Trend Micro has a long history of successfully defending the Exchange environment, consistently leading the mail server security segment on the basis of:

- **Deep Security Expertise.**
  Trend Micro has invested heavily in the TrendLabs global threat-sensing network. Threat experts conduct in-depth research across threat types and vectors to stay ahead of the cyber criminals.

- **Maximum Effectiveness.**
  Rather than continuing to rely on traditional engine-based scanning alone, Trend Micro delivers an innovative mix of technologies and services to thwart increasingly sophisticated attacks. This innovation encompasses expertise gathered and shared across multiple attack vectors, such as messaging, Web, endpoint, and network security.

- **Highly Responsive Support.**
  Customers routinely cite the level of support and information received from Trend Micro as a key benefit. Trend Micro Premium Support gives enterprise customers access to a designated Technical Account Manager who provides proactive, personalized technical support. A wide range of service options enable customers to select the right plan to meet their specific business needs.

- **Total Cost of Ownership.**
  As a result of this established threat expertise, highly responsive support, and maximum effectiveness through continued innovation, Trend Micro reduces the total cost of ownership. A recent independent study by Osterman Research proved that Trend Micro™ ScanMail™ has the lowest TCO with Symantec and Microsoft solutions costing nearly 2 times as much. Read more on the Osterman study.

VI. IT'S YOUR MAIL SERVER!

The threat landscape is more dangerous than ever, largely due to the increased skill of attackers and their strong motivation—the lure of easy money. To stop these insidious threats like NUWAR, TROJ_PROXY, STRATION, or YABE from infecting your network, stick with a proven leader. After all, how critical is email to your business?

As the #1 mail server security software over the past ten years, ScanMail delivers powerful protection that will give you peace of mind. Trend Micro has the technical expertise to implement and maintain effective multilevel protection against emerging and evolving threats. Simply put: ScanMail is your best choice for securing your Microsoft Exchange messaging environment.

To learn more about how Trend Micro can help you meet the challenge, visit www.trendmicro.com or call your local Trend Micro representative.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
USA toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003
www.trendmicro.com