M86 SECURITY

# Today's Blended Threats

## Identifying and Stopping Web-based Email Attacks

### INTRODUCTION

Organizations of all sizes continue to be challenged by increasingly sophisticated security threats. Attackers, motivated by financial gain, are constantly inventing new ways to penetrate corporate defences and access valuable data. Their tools include new zero-day attacks, targeted threats, use of mass variant attacks and now, blended threats initiated via Email. These threats are designed to evade traditional signature-based security products and comprise an ever-growing percentage of malware.

Email blended threats, in particular, have become a popular means of distributing malware. They exploit the "blind spot" and evade typical signature-based anti-virus products by drawing users to websites where new variants of malware are downloaded, often without being initiated by the user. Additionally, these threats are changed frequently to evade the traditional signature-based malware detection used on Web gateways. With current estimates by M86 Security Labs that up to 10 billion blended threats messages being sent every day[1], all organizations—small and large—need a strategy to deal with these ever changing and increasingly more sophisticated threats.

### NEW HACKER MOTIVATIONS

Over the last decade, virus writing has evolved from malicious hoaxes to a thriving and profitable 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, caused minimal damage to companies, other than clean up costs and productivity losses.

However, as with any growth industry, the potential for financial reward has greatly increased the stakes. Today's virus writers are often motivated by financial gain, using malware to steal company data and confidential customer information and like any industry, profit motivations lead to a constant flow of new innovations as attackers look for better ways to get past existing security measures.

Adding to the problem, access to malware has also greatly increased with the ability to purchase attack kits on the Internet complete with documentation and support so that nearly anyone could initiate their own attack and rent time on any one of the growing number of Botnets as a way to send their attack.

### NEW ATTACK VECTORS

Introducing new viruses has, historically, been the simplest way to avoid detection by signature-based anti-virus products. Traditional anti-virus products rely on previous "exposure" to the virus, assigning it a definition or "signature" to aid in future detection. So, virus writers attempt to avoid detection by taking advantage of the time lag for a new signature to be created and placed in a database, also known as the threat window, sometimes taking hours, days, or even longer before organizations are protected from the new attack.

Creating malware variants have also been a successful avoidance technique. Variants of previous malware are easily generated to break existing signatures using automated tools that are readily available, proving to be more than just a nuisance to virus definition writers.

The use of targeted threats has increased dramatically. These Email-based attacks, which are often sent to a very small group of recipients, are designed to circumvent databases and IP reputation services that detect threats based on previously-identified signatures or high volumes of traffic. These targeted threats often appear to come from familiar internal or external sources—such as Microsoft Word™ or PowerPoint™ files, significantly increasing their penetration and infection rate.

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 new attacks. Recent independent research has shown that leading anti-virus solutions catch, on average, only 40% of all malware[2]. Industry experts, including the Yankee Group's infamous report "Anti-Virus is Dead" have predicted huge increases in malware in the coming years[3] .

### BLENDED THREATS

Attackers using alternative channels to breach organizations are now developing blended threats as their new tool of choice. Blended threats use more than one communication channel to initiate and execute a malware attack.

Currently, most blended threats use Email as the initial vehicle to launch the attack, without actually attaching a virus. Malware writers have shifted from attaching malware to an Email to using blended threats: inserting a seemingly legitimate URL link to websites where malware downloads in the background automatically or social engineering is used to encourage the user to not only click on the link but also to allow the download of what is advertised as a new update but in reality is the actual malware.

1 Symantec Internet Security Threat Report, Trends for July-December 06, p. 13.
2 Cyveillance Report Feb 2009
3 Anti-Virus is Dead; Long Live Anti-Malware, Yankee Group, January 17, 2007

A common attack approach may look like this: First, an attacker hacks a legitimate website—often with automated tools—to place the malware. This is a radical change from previous attacks which often came from hastily developed sites set up by attackers, specifically for attack. Other means to deliver malware include SQL injection attacks, the use of malicious advertisements hosting active content on otherwise legitimate pages, iFrame insertions, cross-site scripting (XSS) attacks, search engine and URL redirection. Recent data from one security vendor revealed attacks coming from over 800,000 unique domains in 2008[4] .

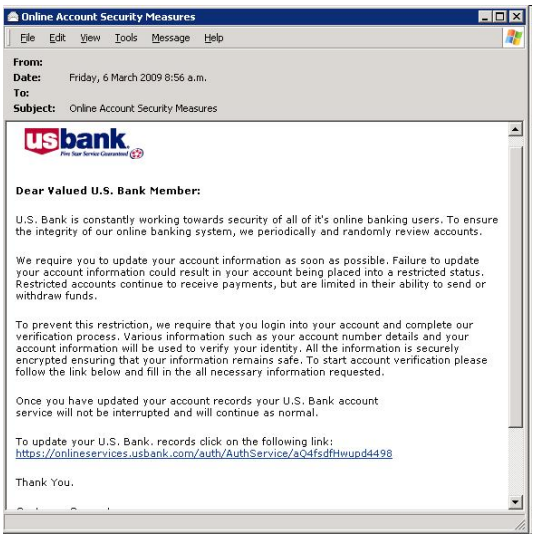
Next, the attacker uses a botnet to send malicious spam messages to end users, often in low volumes to avoid detection. These messages, rather than containing an actual malware attachment, include graphics, URL links, or IP addresses that point to the malicious website. This bypasses traditional Email antivirus gateways which do not identify these features as threats. Finally, assuming the Email passes by spam detection; the user receives the Email and clicks the embedded link, taking them to the infected web page, activating the malware. The malware is deployed as a "drive by download" without any user interaction, or as a result of the user being lured into initiating the installation, often under the pretence of media codec updates, or browser plugins.

Blended threat attacks bypass anti-virus products scanning for malware embedded in Email attachments, and anti-spam engines are proving less effective because the Emails are better formatted and closely resemble legitimate communications. Examples include spoofed Emails from Bank of America (see inset), the Better Business Bureau, and the US Internal Revenue Service.

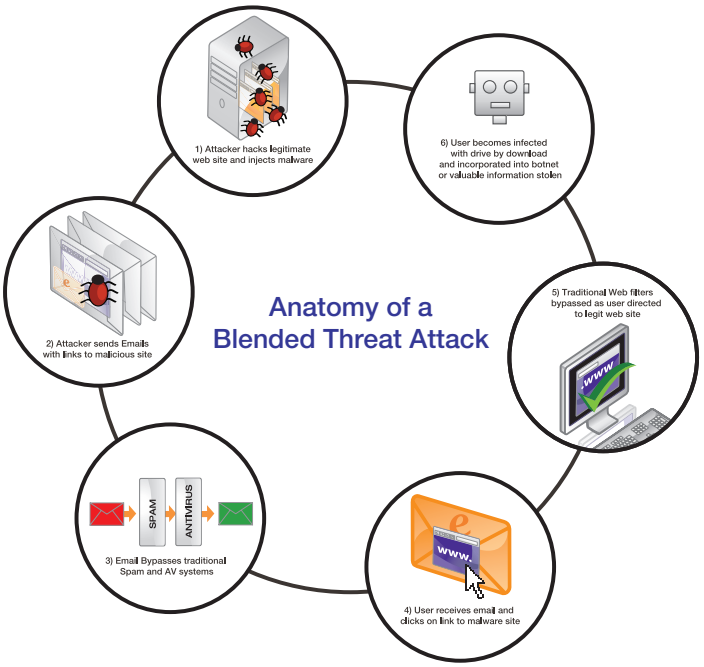
M86's Security Labs found that during 2008 it was not uncommon to see in excess of 30% of current spam traffic containing Web links to malware, making Email blended threats the most commonly encountered type of malicious attack through Email.

Users may even spread these attacks by unknowingly sending or forwarding Emails that contain links to malware inserted into popular Web, social networking and video sharing sites infected with malware. In one such spam campaign surrounding the tragic news about Michael Jackson M86 Security Labs observed this single campaign being responsible for more than 4% of all Spam[5] .

Attackers can also take advantage of product weaknesses and exploit browser vulnerabilities to download malware from websites not blocked by URL filters. Adding to the problem is the growing use of automated tools for finding Web vulnerabilities and the use of SQL injections to infect legitimate websites with malware. In fact, recent estimates are that the vast majority of malware attacks are executed from legitimate websites, including news sites, travel, social networking pages, and blogs. Web security gateways with inbound anti-virus capability are ineffective as the sites often contain polymorphic viruses constantly modifying themselves to avoid traditional signature-based anti-virus applications.




Blended attacks can expose personal or corporate data, incorporate computers into a network of bots and launch other attacks.




## BLENDED THREAT SUMMARY

In summary, Email blended threats are the most recent and dangerous form of malware attacks, because they:

1. Easily evade Email gateway signature-based anti-virus engines by pointing to malicious content on the Web, as opposed to containing malicious content as an attachment.
2. Are enabled through well-designed, structured, and socially engineered Emails
3. Elude most Web filters as they often use legitimate websites to host malicious code and the Web filters do not scan for malware anyway
4. Require no or little user interaction for deployment

4 Web-Based Attacks, Symantec Corporation, February 2009
5 M86 Security Labs Report Q4 2008

## REQUIRED PROTECTION

Blended threats require a solution different from traditional signature-only malware and Web filtering/Email gateway security techniques. This solution must:

- Source Web-based threats by other means other than traditional Web crawling methods
- Provide threat assessment without relying on malware signatures
- Review all Email components, not just attachments
- Observe interactions across communications channels, such as Email and the Web (HTTP)
- Stop the attack at both the Email and the Web gateways

## M86 BLENDED THREAT MODULE

M86 Security, a global provider of integrated, multi-layered Web and Email security products, has developed a solution to specifically protect against blended threat attacks. M86's Blended Threat Module utilizes cloud-based behaviour-analysis technology that works in conjunction with M86 products, including MailMarshal SMTP, WebMarshal and the R3000 Internet filtering appliance. This patented technology complements existing security solutions by detecting threats that cross over between Email and the Web.

M86's approach is unique because it safely observes the actual behaviour of potentially threatening links found in messages, rather than relying on reactive signature-based approaches. The Blended Threat Module in MailMarshal SMTP firstly checks any suspicious links against the locally cached copy of the blended threats knowledge service, if still unknown it forwards the suspicious link to the cloud-based Blended Threat Knowledge Service for analysis and identification. The cloud service also includes URL databases updated by M86 Security Lab analysts and other proprietary messaging sources, providing an additional means to identify potential threats on the Web. These threats are automatically and proactively analyzed to observe the actual behaviour of the message or content in a secure and protected environment.

These confirmed threats are submitted to the Blended Threat Knowledge Service. This service is then fed back and integrated into M86's Web products—such as the R3000 Internet filter and WebMarshal—to provide accurate, reliable protection against blended threats across Email and Web.

The analysis engine behind the Blended Threats Knowledge service observes the behaviour of potential blended threats with the behavioural observation engine, reviewing the active content and even activating links to the embedded 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 blended threats. Because the Blended Threat Module doesn't rely on signatures, it provides a critical layer for catching and neutralizing new exploits.

The changing nature of malware threats requires new, smarter solutions to protect users from attacks. M86's Blended Threat Module is uniquely capable of blocking the advanced threats faced by companies today.

## BENEFITS

Unlike other anti-virus products, M86's Blended Threat Module proactively blocks blended threats and blocks even new attacks and malware without signatures.

The benefits of the Blended Threat Module include:

- **Block threats in Email** – with the advent of blended threats in Email a lot of trust has gone from using URL links in legitimate Email messages. The Blended Threats Module blocks the Email before it reaches the user stopping the threat before it reaches the inbox and giving users higher peace of mind.
- **Rapid response to new attacks** – Blended threat attacks often utilize legitimate websites and last for only a few hours. The Blended Threats Module utilizes cloud-based real-time detection, stopping the threat as it happens.
- **Accurate malware detection** – Blended threats most often use new malware variants in order to bypass signature-based malware scanning solutions. The blended threats module uses behavioral analysis technology to detect new variants to protect from internet borne malware and malicious links.
- **Around the clock protection** – The blended threats service operates 24x7 consuming information and suspect links from M86's extensive customer base Email and Web security solutions and other feeds monitored by M86 Security labs and the specialist threat analysts.
- **At-a-glance console integration** - The Blended Threat Module integrates seamlessly into MailMarshal SMTP interface, allowing administrators to track blended threat attacks in the MailMarshal console.
- **Zero administration** – Once configured, the Blended Threats Module is completely autonomous and self-contained, requiring no ongoing administration.
- **High value threat protection for little additional cost** – The Blended Threats Module can be purchased as a low-cost addition to yearly product maintenance or your yearly malware subscriptions.

## SUMMARY

As attackers become more sophisticated, the use of new tools, such as blended threats, has increased—compromising valuable financial and personal information. The use of malicious (and legitimate) URLs and active content in Email are undetectable by traditional anti-virus products, whether they are running at the Email gateway or the Web gateway. The addition of blended threat protection to M86's product line makes it uniquely capable of stopping these new threats quickly and effectively, before they reach the end user.

## ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.com.

## TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**

M86 SECURITY™

**Corporate Headquarters**
828 West Taft Avenue
Orange, CA 92865
United States

Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

**International Headquarters**
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848080
Fax: +44 (0) 1256 848060

**Asia-Pacific**
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 10.23.09