



Businesses Beware: The New Battlefield on Web and Email Attacks

“Email and the Web offers colossal productivity benefits. But it also poses areas of risk that can threaten productivity, system uptime and the reputation of your organization. New external threats like phishing and spyware need more than traditional anti-virus defences.”

Table of Contents

The new cyber crime endemic	4
From blanket bombing to calculated sniping	4
As if viruses, worms and trojans weren't trouble enough	5
The new battlefield: The Convergence of Email and Web Based Attacks	5
Gone phishing	6
Are you being watched?	6
The true costs to business	7
Certainty in all business information exchange	8
MessageLabs Email Protect	9
MessageLabs Web Security Services 2.0	9
The bottom line	10

External threats now take the form of 'under the radar' approaches designed to get past traditional security tools.

Introduction

Gone are the days when viruses simply corrupted your network, costing your organization time and money to clean up the damage. Today's threats consist of 'under the radar' approaches in the form of multi-vector attacks, which operate across email and the internet and are designed to get past traditional security tools.

Email and web-based attacks like phishing and spyware are costing business and consumers loss in productivity and system downtime, financial losses, as well as and brand damage.

This white paper examines the nature of the new threats, what they're designed to achieve, and their true costs to business.

It examines the alternatives available to combat them: appliances, software and Managed Services. It assesses their strengths and weaknesses, and their relative total cost of ownership.

The need for creating certainty in all our exchange of electronic information is clear, whether this is across email, the internet, VoIP or instant messaging. Achieving it, without hampering the speed and continuity of business over the internet, requires some doing. Businesses today have a clear need for real time internet-level protection from known and unknown email and web-based threats.

The indiscriminate mass mailing of virus infected code is fast being replaced by targeted attacks that use 'tricks' to bait the hook against individuals and organizations.

The new cyber crime endemic

More and more of our communication is becoming computer-based, whether this is via email, the internet, VoIP and instant messaging. And as our organizations become more networked, we open up more and more avenues for cyber criminals.

In 2004, for the first time the proceeds of cybercrime – estimated at more than \$105 billion - surpassed the underworld's profit from illegal drugs. Organized crime is finding a ready source of chinks in our complex, but often haphazard and reactive, electronic defences.

From blanket bombing to calculated sniping

The indiscriminate mass mailing of infected code is fast being replaced by targeted attacks that use 'cyber tricks' to bait the hook. Online crime is evolving rapidly – and fast becoming more sophisticated and widespread, more determined and devious. And as attacks become more targeted, they're more effective.

Its most recent and most powerful manifestation is the multi-vector (or blended or hybrid) attack. Vectors are all the various modes connections a computer can make – and thus the various ways malicious code can infect your organisation. Vectors include email (SMTP), web browsing (HTTP), instant messaging, peer-to-peer networks, file sharing and Wi-Fi.

An example of a multi-vector attack involves an email entering an organization and then enticing an unsuspecting user to activate an embedded link to a malicious website that infects the targeted network or computer. The attack jumps from one communication protocol to another, such as from SMTP to HTTP or IM.

Due to the level of stealth-like approach of these multi-vector attacks, it is far more difficult for traditional security software solutions to identify and remedy these approaches in real-time. The bottom line result is that your employees within your organization could be at risk without you or them realising it, causing the potential for lost productivity, system downtime or financial loss.

The automatic jump across vectors hugely magnifies the effect – and cost – of each attack.

As if viruses, worms and trojans weren't trouble enough

Before the advent of multi-vector attacks, cyber crime came in three basic shapes: viruses, trojans or worms, which infect a computer and then propagate, choking bandwidth and disabling networks. Viruses and worms can also carry payloads – from irritating messages to highly destructive, costly commands, such as rolling back security measures and corrupting databases.

Viruses

Viruses, such as the long-lived Netsky and Mydoom, are self-replicating code that spread between applications and latch onto essential system files. A user needs to trigger a virus by completing a specific action – most commonly opening an email attachment. Whereas in their first iteration viruses were mainly spread through infected floppy disks, over 85 per cent of all viruses are now spread via email.

Worms

A worm, such as the SQL Slammer or Blaster, is a software program that replicates itself across a network, spreading between services. It can self-execute without a user's intervention, and often lodges only in memory, avoiding detection by file-scanning antivirus software by staying out of the file system.

Trojans

Trojans, like the ancient wooden horse filled with murderous Greek warriors, appear harmless or even useful. They disable firewalls and antivirus software to avoid detection, and actively conceal their outbound connections. The user believes they are downloading a screen saver or piece of software. In fact, they've invited in an unseen enemy, content to wait silently, monitoring a network or providing a backdoor into the system later. For example, the well-known Trojan masquerading as a screen saver installed the spyware Perfect Keylogger.

The New Battlefield: The Convergence of Email and Web Based Attacks.

Unlike viruses, worms and trojans, which have a single mode of infection and usually require user activation, multi-vector, hybrid or blended threats spread in multiple ways, using email, instant messaging and peer-to-peer networks and exploiting web browser vulnerabilities. Multi-vector attacks are designed to evade single point security solutions and propagate as fast as possible. The huge rise in spam rates – estimated at between 60 and 77 per cent of all emails – combined with our increasing everyday use of the internet – makes us particularly vulnerable to the new multi-vector attacks.

Passwords, account details, credit card numbers, usernames and file data are all automatically collected, on a massive scale.

Gone phishing

Phishing is one of the most prevalent forms of a multi-vector attacks – and it is on the rise. Phishing, and its even more targeted variant, spearphishing (targeting specific individuals within an organisation such as the finance director or CEO), is nothing more than a traditional confidence trick. But its criminal power is increased exponentially by the power of the internet through the use of spam.

Fake websites that are near-perfect replicas of a real business's website – except for a slightly incorrect web address and a missing or invalid digital certificate – are posted on the web. The criminals then unleash millions of spam emails, which also replicate the business's official communications. The spam directs recipients to the fake website and asks them to log in, providing confidential passwords and financial information. The replicas are so convincing that the Anti-Phishing Working Group estimates that around 20% of recipients click on the links, and 5% actually enter their confidential information.

The information can then be used to make illegal transactions, stealing from the spam recipient or from the business that has been used as bait. Or it can be on-sold to another criminal organization.

Are you being watched?

Another example of a multi-vector attack at its most extreme centers around the installation of spyware, ranked as the second worst threat to enterprise network security in IDC's 2005 *Enterprise Security Survey*, and estimated by IDC to account for up to 30% of all helpdesk calls, with 67% of all computers having some form of spyware – in most cases, multiple programs.

Spyware is any software application that secretly gathers information about the computer user and sends it on to another user via the internet. Users can unknowingly download spyware from websites, through file attachments or through 'auto-install' applications. Traditional antivirus solutions cannot detect spyware, as they cannot 'catch' the self-propagating properties of spyware.

Spyware can simply cause annoyance and lost productivity through pop-up ads, consuming bandwidth and draining IT resources – or it can be put to devastating use by cyber criminals. In many cases, staff frustrated and annoyed by continual pop-ups generated by spyware, download pop-up blockers which themselves contain malware.

In some multi-vector attacks, spyware that secretly installs a keystroke monitor is distributed via spam. The keystroke monitor forwards everything that is typed on the keyboard to the criminals. Passwords, account details, credit card numbers, usernames and file data are all automatically collected, on a massive scale.

With an even greater potential to cost business dearly, some spyware can interrogate the system on which it's lodged, opening confidential files and uncovering network passwords – placing at risk an entire corporate intellectual property, as well as lost productivity and the time and cost of disinfecting a network.

The risks to business range from financial losses, system downtime, lost productivity and damaging publicity.

The true costs to business

We're increasingly dependent on the internet for corporate communications and storing and managing confidential information. The benefits are enormous. Yet every connection brings a world of risk right through your new electronic front door. Your network security needs to protect more than your computers and your IT budget – it's there to safeguard your intellectual property, your reputation and your bottom line.

Downtime

Every day, information security threats to disable business networks – from state and federal government organizations to small suburban businesses. They're costly to clean up, productivity plummets while the computers are down and you can even lose sales.

Confidentiality

Every business stores data that needs to be securely kept behind closed doors. A multi-vector attack can access your confidential corporate or customer information, without your knowledge. Used for criminal activities including identity theft and fraud, the risks to business range from financial losses and higher insurance premiums, to damaging publicity and loss of goodwill.

Legality

Government and industry regulations are placing unprecedented pressure on corporations to secure their electronic communications, and laxity can invite criminal and civil penalties. Inappropriate content, sometimes a factor in multi-vector attacks, carries liability risks for employers, who have a duty of care towards their employees. And if one of your employees uses your corporate email server to despatch a batch of spam, your business can be held liable for their actions.

Defending electronic communication channels

Industry estimates, reported in IDC, put daily global emails at around 80 billion – and the proportion of them that are spam at a staggering 77%. And we couldn't work without the internet – it's become a virtual shop front for many businesses, but unsecured websites are a breeding ground for multi-vector attacks, primarily phishing and spyware. Research by IDC in 2002-2004 found that 30-40% of web access at work had nothing to do with the employee's job, resulting in security, productivity and legal risks.

We need the information superhighway to flow fast without impediments or roadblocks, yet rigorous security and thorough checking of every load it carries is vital.

While there is anti-spam and cyber crime legislation, legal controls have limited effect as most spammers use off-shore email domains to transmit spam, and illegal techniques like address spoofing, trojans and the bot-net to conceal their identity.

The only real answer is for all businesses, large and small, to implement a cost-effective and multi-layered approach. The first essential step is the installation of real time protection at the internet server and desktop levels. Secondly, the introduction of a coherent and enforceable email and internet security policy to enforce practical measures to guard against damage to the information communication system. The third and final step is critical, yet often neglected. All employees and users need to be educated about information security on an ongoing basis. Security rules will not be kept without ongoing, active review and staff training. Staff also need to be reminded that their email and internet use can be monitored, so they can protect their own privacy.

A Managed Service ensures a team of experienced information security specialists and massive processing power is always on hand to ensure seamless, real-time protection.

Certainty in all business information exchange

Maintaining business continuity is critical, no matter what your business. A technological defence against known and unknown information security threats is the key element in any email and internet security policy.

Businesses can choose from a myriad of tools, which fall into three broad categories: appliance, software and Managed Service. Confusion exists in the marketplace about which of the three categories provides the most effective protection, and what the true total costs of ownership are.

Appliances

The appliance is a hardened server installed between email and internet server and network boundary, requiring set up and configuration to match the settings to the business's email and internet environment. As download volumes, bandwidth and security needs grow with a business, additional appliances need to be purchased to expand the network security capabilities.

Material must be downloaded onto the corporate server before an appliance can check it for infection. While the appliance is carrying out checks, bandwidth is compromised and systems are slowed.

With appliances, in-house information security expertise is essential to monitor malware trends, adjust appliance settings, configure updates, maintain and manage appliances, manage demands on storage and bandwidth and provide support to users. Moreover, additional redundant appliance hardware can be necessary to ensure business continuity in case of system failures. The total cost of ownership of an appliance solution invariably extends beyond the initial purchase price to include the cost of more than one dedicated, specialised IT specialist – which usually translates into a high opportunity cost for appliance solutions.

Software

Licensed security software is installed between the email and internet server and the network boundary, which often requires specific server hardware and software, adding to the infrastructure complexity. The effectiveness of a software solution is then totally reliant on it being kept up to date with the latest signatures to combat the escalating tide of emerging threats and unknown attacks. This presents significant ongoing total cost of ownership increases.

The public nature of software solutions can even work to undermine their effectiveness, as cyber criminals continually evolve their malware to work around security software.

Managed Service

While appliance and software solutions represent first generation information security solutions, their escalating and unpredictable costs and increasing scalability and performance problems have presented businesses with further challenges.

Table 1 shows that, in contrast to appliances and software, a Managed Service identifies threats *outside* the corporate network, at the internet level, and removes unwanted content and attacks before they enter a business's network. With no hardware or software required on your premises, there's no need for maintenance, and no complexity added to your infrastructure. Costs are fixed, with a single point of support around the clock.

With the growing need for in-depth knowledge to keep up with increasingly devious and targeted multi-vector attacks, a Managed Service ensures a team of experienced information security specialists and massive processing power is always on hand to ensure seamless, real-time protection – at the lowest total cost of ownership.

**Table 1:
Comparative features for the three categories
of web and email protection**

Features	Managed	Appliance	Software
Quick and easy setup	●●●●●	●●●●●	●●●●●
Predictable cost/low TCO	●●●●●	●●●●●	●●●●●
Load balancing and redundancy	●●●●●	●●●●●	●●●●●
Platform OS independent	●●●●●	●●●●●	●●●●●
No maintenance required	●●●●●	●●●●●	●●●●●
Reduced bandwidth cost	●●●●●	●●●●●	●●●●●
Transparent signature updates	●●●●●	●●●●●	●●●●●
Transparent engine updates	●●●●●	●●●●●	●●●●●
Quarantine off-site	●●●●●	●●●●●	●●●●●
Disaster Recovery	●●●●●	●●●●●	●●●●●
Scalable	●●●●●	●●●●●	●●●●●

●○○○○ Straggly disagree/Feature not offered
 ●●○○○ Straggly agree/Perfect match
Note: Data based on MessageLabs research and competitor marketing material

MessageLabs Email Protect

MessageLabs Email Protect services combat all threats, including multi-vector attacks and the new generation of attacks criminals will unleash in the future. Email Protect ensures that spam never reaches your corporate network, eliminating it on the internet in real time before it can bring malicious payload onto your system.

Email Protect services are multi-layered, combining best-of-breed technology and techniques with MessageLabs' proprietary Skeptic™ predictive technology.. Benchmarked by VeriTest to be 99.61% effective, meaning it will stop almost all incoming spam emails before they enter the organisation. At the same time, Email Protect has a negligible false positive rate of 0.04%.

Email Protect incorporates MessageLabs' anti-virus service, which prevents all known and unknown viruses reaching your network, and our content filtering service, ensuring inappropriate and offensive content cannot be downloaded, thereby protecting businesses from very real legal liability risks.

MessageLabs Web Security Services 2.0

MessageLabs Web Security Services comprise Anti-Spyware and Anti-Virus to protect organizations from 100% of spyware and malicious content, and a highly configurable Web URL Filtering, enforcing acceptable web use policies, keeping employees safe and productive and ensuring regulatory compliance.

Multiple commercial virus scanning engines identify known viruses, and proactive web heuristics protect against unknown web viruses, scanning web traffic for the features associated with suspicious activity. Threats are then isolated and neutralized before reaching your network.

Because the multi-vector attack arrives in the form of a hyperlink contained in a piece of spam, the spam email contains no actual malware for software and appliance solutions to detect. MessageLabs Managed Service follows the link before the spam hits your corporate boundary, and checks the site for spyware before it can reach unsuspecting users. In 2005, 12,000 attacks prevented by MessageLabs were not identified anywhere else.

MessageLabs provides industry-leading Service Level Agreements on availability, latency and protection. Comprehensive reports and audits can be generated on demand, and an email alerting feature notifies administrators and users when threats are detected.

The user and web manager experience is critically important. MessageLabs Managed Service is globally load-balanced to ensure stability, speed and redundancy, and operates through a 'one window' management interface with 24/7 worldwide service and support. With MessageLabs working in real time, users experience no noticeable delay in their web browsing.

Benchmarked by VeriTest to be 99.61% effective, MessageLabs was placed as a leader in Gartner's June 2005 Magic Quadrant.

With unprotected computers estimated to survive 30 minutes on the internet, email and web security is of absolutely paramount importance.

The bottom line

It's not only business that benefits from the limitless potential of the internet – organized crime has now discovered its power, and turned enormous resources to undermining business's and consumers' efforts to protect electronic communications.

With unprotected computers estimated to survive 30 minutes on the internet, email and web security is of absolutely paramount importance. Moreover, the complexity, cunning and changing nature of the new multi-vector attacks – and their power to wreak financial havoc – means that specialist information security expertise needs to be on hand, up to date and staying one step ahead.

Managed Services provide businesses with a team of experts and unparalleled technological power, at a predictable and controlled cost. MessageLabs, an industry leader, guarantees unmatched Service Level Agreements, ensuring productivity, compliance, business continuity and protecting businesses from the latest, most dangerous and complex multi-vector threats – and the new threats the future will bring. On the new battleground, business needs the good guys on their side.

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
FeringasträÙe 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

© MessageLabs 2005
All rights reserved

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300