MessageLabs – Managed email Security

AVAR 2003 - November 2003

Agenda

- Corporate Overview
  - About Us
  - Email Threats
- The MessageLabs Service
  - ***Anti-Virus***
  - **Anti-Spam**
  - Anti-Porn
  - Content Control
- Our Technology
  - Skeptic Architecture
  - Our Difference

Organization Structure

star technology group

MessageLabs — Star

- Part of Star Technology Group (www.startechgroup.co.uk)
- 400 employees
- Global presence
- High quality investors
- $60 million run rate revenues

MessageLabs Profile

- The Leading Provider of Managed Email Security Services for Businesses Worldwide:
  - Global Presence (Americas, EMEA, Asia Pacific)
  - 5500+ Business Customers Globally
  - 99% Customer Retention Rate
  - More than 18mm Daily Emails Scanned
  - 200+ Employees
  - Membership in Wildlist.Org, Anti-Virus Information Exchange Network (AVIEN)
  - Inherits Star's ISP Network Skills

Security / Expert Credentials

- ISO 17799 / BS 7799 Certification
  - Employee background checks
  - Restricted access to systems
  - Periodic Security Audits
- Clients include Government and Quasi-Government Departments and Agencies
- Alex Shipp – Articles published in Virus Bulletin. Quoted on CNN, BBC News, CNET News, Internet Security News, ZD Net, The Register, Computer Security Now, and others.
- Matt Sergeant – Speaker at MIT Spam Conference, FTC Spam Forum. Lead Spam Assassin Developer. Quoted in BBC News, Computer Weekly, Internet World, and others.

Some of MessageLabs Customers

Federal Reserve Bank · Lloyds TSB · Jackson Walker L.L.P. · The Bank of New York · SallieMae · INA Insurance Group of North America · Dorsey · Brown Raysman · Bank of the West · Briggs · Marlborough Stirling · Strong · Daiwa · Fenwick & West LLP · Andrews Kurth · GMAC RFC · London Stock Exchange · FTD.com · Brocade · The Condé Nast Publications Ltd. · The Vital Ingredient · AES Corporation The Global Power Company · MeadWestvaco · symbol · Purdue · Fujitsu · Red Wing Shoes · FMC · BIC · 10 Downing Street · Viacom · Incepta · Moen · Air Products · Manpower · Paul Mitchell · SC Johnson · Rentokil Initial · mitsubishi

The MessageLabs Network

MessageLabs: A Truly Global Architecture

- Network of 'Control Towers' – Redundant Towers for Failover Resilience
- Full Scalability – Add More Towers As Needed
- Only Service With ISO7799 (BS7799) Certification!

US Infrastructure is also growing with our business

- We now scan over 23 million emails a day, 100+ million a week.
  - 42+ towers
  - 800+ servers worldwide
- MessageLabs has 42 email scanning towers worldwide in the following locations:
  - USA
  - UK
  - Germany
  - Hong Kong
  - Amsterdam
  - Australia
- Australian facility online November 2003

What is a MessageLabs Control Tower?

- A Control Tower is a 7 foot high rack that contains:
- Up to 26 Mail Servers running:
  - Qmail on RedHat 8
  - 3 Virus Scanners
  - Skeptic
- Various pieces of networking equipment:
  - Load Balancers
  - Switches
  - Management Components
- Other Components:
  - SQL Servers

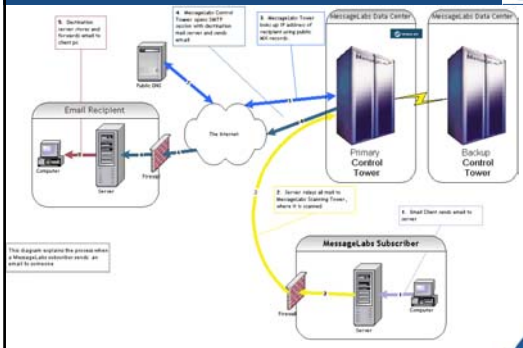
What is a MessageLabs Control Tower?

- Cisco 3640 or Cisco 7204 VXR Router
- Cisco Catalyst 2924XL Fast Ethernet Switches
- 2 Cisco Local Directors (LDIR 416)
- Services Server - Provides DNS services to the other servers
- Monitor Server - Distributes control files, signatures and software to the mail servers
- 26 Compaq DL360 Mail Servers - Run RedHat 8, qmail, 3 virus scanners and Skeptic™
- 2 SQL Servers - Run Windows NT4 and MS SQL Server
- A TNG Server - Runs Windows 2000 Professional and CA Unicentre TNG
- Some Power Distribution Units (PDUs)

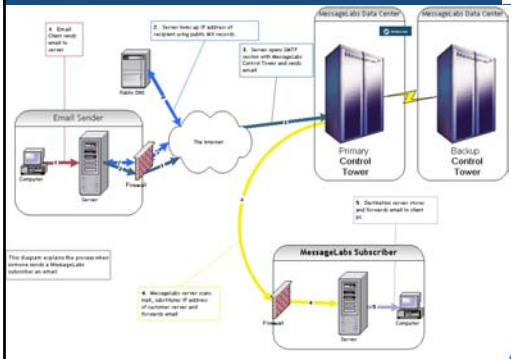
How does one use the service?

- Inbound Mail
  - Redirect your MX records in DNS to the MessageLabs Network.
  - We will scan the mail and forward it to your SMTP server
- Outbound Mail
  - Configure your mail servers to forward mail to the MessageLabs Network
  - We will scan the mail and deliver it to the recipient

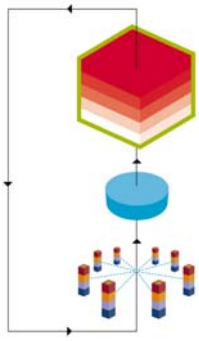
Outbound Logical Flow



Inbound Logical Flow



Unique Technology



SKEPTIC

- *Identify threats proactively*
- *Works off a knowledge base of rules*
- *Thresholds are set and action taken*
- *Knowledge base is constantly learning*
- *For the dynamic and changing nature of email security threats*

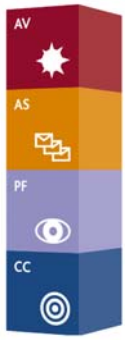
Skeptic™: The Secret of Our Success

- MessageLabs' Proprietary, Patented Heuristic Scanner
- Focused on Identifying Unknown, Dynamic and Changing Email Threats
- 4+ Years of Development Time
- More Than 5 GB of Heuristic Rules
- Rapid Application Development Architecture
- Utilizes Instant Updates
- Contains a Large Database:
  - Virus "DNA"
  - Known Security Vulnerabilities
  - Spam Detection Rules
  - Image Composition Analysis and Common Objects for Image Identification
- Detection Based on Scoring System for Each Email Threat
- Able to unpack virtually all data packing formats

SKEPTIC

Service Overview

- Anti-Virus
- Anti-Spam
- Porn Filtering
- Content Control



MessageLabs: Anti-Virus

No more viruses

The MessageLabs anti-virus service uses multiple scanners and Skeptic patented artificial intelligence to detect and stop all viruses, known and unknown, before they reach you.

The service comes with a unique 100% Service Level Agreement in applicable countries as proof of it's unrivalled effectiveness.

Current solutions

- Existing AV scanners rely on signatures
  - Signatures take time to produce
  - Signatures **cannot** catch unknown viruses
- Virus writers practice against commercial products
- Existing products require large overhead on servers

Signature-Based AV Risks

- GAP 1: Time between when a new virus is released and when the antivirus vendor creates a new signature
- GAP 2: The time between when the new signature is created and when enterprises receive signature files and implement the update at every desktop

Gartner

Twin "Achilles' heels" of signature-based antivirus – Gartner, August 31, 2001

Independent Anti-Virus Lab Testing

Independent Anti-virus Lab Testing		
PC Magazine April 22, 2003		
Virus Accuracy Testing		
Eset Software	93%	
Network Associates	69%	
Panda Software	83%	
Sophos	83%	
Symantec Corp.	97%	
Trend Micro	92%	

Results compiled from February 2001 to February 2003 from AV-Test.org, ICSA Labs and Virus Bulletin's VB100 certification. The tests challenge a product to catch every current virus in the wild (in circulation) and not report any false positives

Independent Anti-Virus Lab Testing

Independent Anti-virus Lab Testing		
PC Magazine April 22, 2003		
Virus Accuracy Testing		
Second Tier Vendor A	93%	
First Tier Vendor D	69%	
Second Tier Vendor B	83%	
First Tier Vendor C	83%	
First Tier Vendor A	97%	
First Tier Vendor B	92%	

Results compiled from February 2001 to February 2003 from AV-Test.org, ICSA Labs and Virus Bulletin's VB100 certification. The tests challenge a product to catch every current virus in the wild (in circulation) and not report any false positives

Phase One: Reactive Scanning

- 3 Commercial Scanners:
  - F-Secure
  - NAI
  - V-find
- Updated every 10 min. via static links

F-SECURE MCAFEE CYBERSOFT

Phase Two: Skeptic (Proactive Scanning)

- Skeptic Code Analysis
  - Determine behaviour of an email
  - Detect replication schemes
  - Reverse virus scanning
  - Startup code analysis
  - Cryptographic analysis
- Filename and file type analysis (~250 types)
- Searches for virus-like behaviour
  - Duplication (file activity, mass mailing, MIRC)
  - Payloads (mass deletion, unusual trigger conditions)
  - Obfuscation
  - The more the virus authors try and hide from signature scanners, the more the code stands out to Skeptic

SKEPTIC

Phase Two: Skeptic (Proactive Scanning)

- Scores email according to a set of rules:
  - Mail containing office-macros/exe files sent to more than 20 recipients (100 points)
  - Mail from well known virus sending domains (e.g.Bulgaria) (20 points)
  - Mail containing executable code within HTML sections (70 points)
  - Mismatched message headers (50 points)
- If the email scores more than a threshold value, the message will be quarantined

Protecting Against New Outbreaks

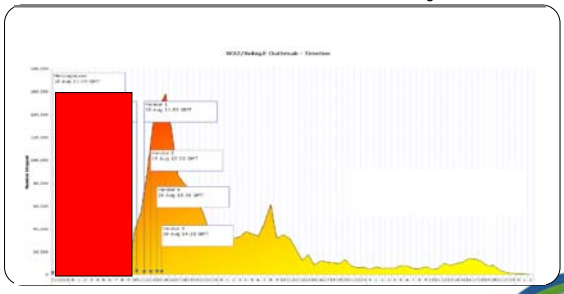
- The first AV company to discover a new virus gets to choose the name, and so it is no surprise that most of the mass mailers of recent years were named by MessageLabs:
  - LoveBug
  - Goner
  - Klez
  - Fizzer
  - SoBig
  - Ganda
  - …to name but a few. (the full list is quite big!).

Guard Against the Blended Threat

- Viruses such as Fizzer, Bugbear and Sobig are all known to install backdoor trojans
- These Trojans are used to take control of the machine in some way, and in this case, to be used for sending spam.
- Spam messages containing backdoor-trojan attachments are being sent in large volumes

Proactive Threat Defense

Outbreak of the 'SoBig.F Virus in 2003



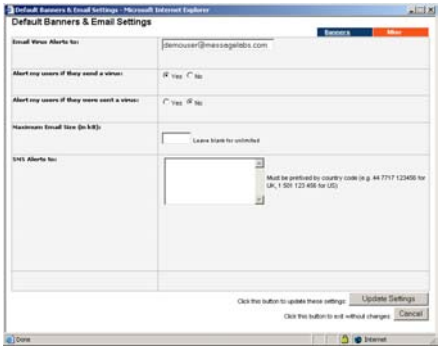
- MessageLabs Customers Were 100% Protected
- Not One Infected Email Reached a Customer's Network

Actions Taken on Viruses

- When we intercept a virus either leaving your network or trying to enter your network, the following actions take place:

1. Virus email is moved to MessageLabs Virus Quarantine for 30 Days
2. Notification email sent to designated Administrator at client and Optionally…
   1. Email alert your users if they send a virus
   2. Email alert your users if they were sent a virus
3. Administrator has option to release email to recipient

Actions Taken on Viruses



Anti-Virus Differences

- 100% Virus-Free email
- Only service to provide proactive virus detection through Skeptic
- 30 Day Virus Quarantine with no size or storage limits
- Stop the Virus before it ever reaches your network!

MessageLabs: Anti-Spam

Reduce spam dramatically

The MessageLabs anti-spam service uses a combination of Skeptic technology and customer configurable blacklists/whitelists to identify and re-route spam before it reaches you.

In a recent independent evaluation, this highly effective filter mechanism came out as the clear leader in terms of filter accuracy (96.4% Effective with 0.04% False Positive Rate)

The Spam Threat

- MessageLabs detects over 3 million Spam messages every single day - (*MessageLabs Intelligence - May 2003*)
- As a percentage of our volume incoming spam is 45-55%- (*MessageLabs Intelligence - May 2003*)
- Growth rate of 200-300% year on year
- "AOL blocking 2 billion spam messages a day"

New Developments in Spam

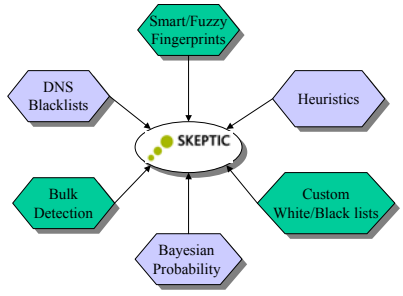
- Open Proxies
- Dictionary Attacks
- Spam+Trojan Combo
- Statistics Busters
- Hidden HTML
- Slice and Dice

Anti-Spam Techniques

- DNS Blacklists (MAPS) – Not very effective
- Naïve Content Filtering – Key Word Search And Block
- "Simple" & Fuzzy fingerprints – Spam Snapshots
- Heuristics – Rules Based Analysis
- Statistics and AI techniques – Bayesian Analysis
- Challenge/Response – Flawed
- Collaborative Filtering – Razor, Cloudmark

Why our approach works

- We take the best of breed and combine them



Heuristic Rules

- Scoring system based on 1200+ rules
  - Accept Credit Cards **+1.00**
  - Subject: is empty or missing **+1.40**
  - Contains 'G.a.p.p.y-T.e.x.t' **+1.00**
  - Claims not to be selling anything **+1.49**
- Other Heuristics Rule Classes
  - RFC 2822 violations
  - Forged headers
  - "Click here" URL
  - Pornographic words
  - Ratware fingerprinting detection
  - List removal instructions
  - Spam phrases
  - Known spam scams

Heuristic Rule Training/Testing

- Over 20GB of training/testing emails
- System automatically re-weights scores based on training data (using a genetic algorithm)
- Rules added/removed as required

Bayesian Probability (Statistics)

- Technique that looks at the probability of words or phrases (tokens) being found in spam or non-spam emails.
- Each token is assigned a probability based on it's occurrences in a sample of spam and non-spam email
- When a new email is processed the individual probabilities are combined to give an overall percentage chance that an email is spam.
- A calculation is made:
  - spam is given a positive score
  - non-spam is given a negative score
  - emails that the statistical analysis is unsure about are given a zero score.

Public Black Lists

- **ORDB**: Open Relay Database. ORDB.org is a non-profit organization which stores a IP-addresses of verified open SMTP relays. These relays are, or are likely to be, used as conduits for sending unsolicited bulk email, also known as spam.
- **RBL**: Real time Black hole list, a list of known spamming domains, I.e. those which have already been used to send spam
- **RSS**: Relay spam stopper, another version of ORDB
- **DUL**: Dial up list, A list of IP addresses associated with dial up accounts, normally users with dial up account send email from their ISP's mail server, there is a high probability that any mail being sent directly from a dial up IP address is spam.

Custom Black & White Lists

- Customers can add domains, email and IP addresses to their own black and white lists
- **Black Lists** – Mail matching any of the criteria here will be acted on as designated by customer. (Block & Delete, Redirect, Tag)
  - Mail from unwanted senders
  - Ex-employee / competitor communication
- **White Lists** – Specifies mail to not be scanned for spam. Mail that looks spammy but is not.
  - Obscure Newsletters
  - Ad Filled Order Confirmations
  - Wanted Spam

ML DNSBL

- Multi-source DNS black/whitelist
- Actively blacklist spewing IPs
- Active proxy/relay scanning based on "spam in hand"

MessageLabs Spam Fingerprints

- We take spam collected from the Spamtraps and turn it into a 192 digit number or Fingerprint
- Then, when an email is scanned we can:
  - Turn it into a 192 digit number
  - Compare it with our known fingerprints
  - Reject it as spam if it matches
- Body, Fuzzy Checksum, URL and URL IP fingerprints

Bulk Detection

- Fingerprint all email (using fuzzy checksums) and storing counts
- Automatic bulk detection allows us to instantly block "bad" fingerprints
- Skeptic Radar for Spam

Actions Taken on Spam

- When Spam is identified, the following actions can be taken:
- Append a header and allow mail through
- Append a header and redirect to a bulk mail address
- Block and Delete
- Actions are selectable by detection technique:
  - Heuristics, ORDB, RBL, RSS, DUL, Custom IP Blacklist, Custom Domain Blacklist

Anti-Spam Differences

1. Most accurate filtering of Spam
2. Lowest false positive rate when filtering Spam
3. Pro-active filtering not reliant on public lists
4. Uses Artificial Intelligence / Heuristic engine that continually "learns" and Bayesian Algorithms to identify Spam
5. No end-user involvement required
6. Tag, Re-direct or Block Spam before entering enterprise

PC Magazine

Corporate Antispam Tools

February 25, 2003
By Richard V. Dragan

MessageLabs AS

MessageLabs "yielded the best results on our tests, producing the cleanest in-boxes of any solution."

PC MAGAZINE

MessageLabs: Complete Email Security

Control your content

The MessageLabs content control service uses Skeptic technology to identify confidential, malicious or inappropriate content according to your settings.

Content Control

- Expected Q4 2003
- Allows companies to scan for unacceptable content and attachments
- Scan by attachment type (scripts, executables, graphics, media)
- Scan by attachment size, restrict the number of attachments
- Scan by Lexical Analysis
- Auto-Zipping
- Can Block, Copy Admin, Redirect to Admin or Tag

Reporting and Administration

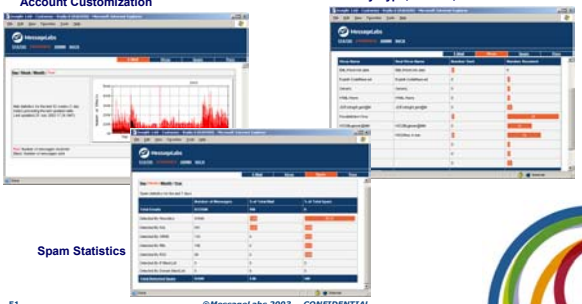
MessageLabs InSight

MessageLabs Insight™

Proprietary Web-Based Account Management & Reporting Tool

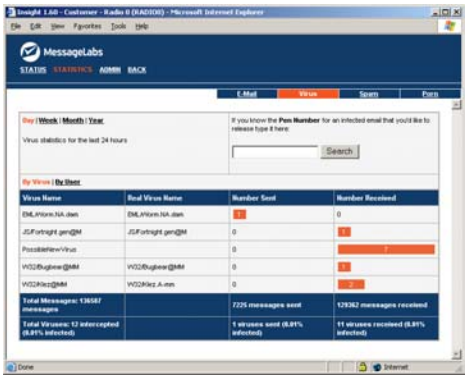
Activity Reporting
Account Customization

Virus Statistics
by Type, Sender, etc.

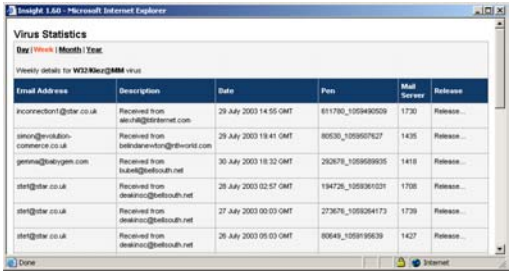


Spam Statistics

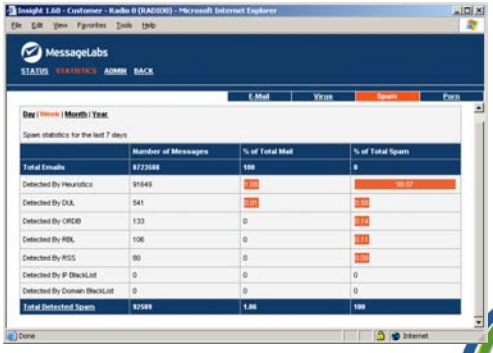
Virus Statistics



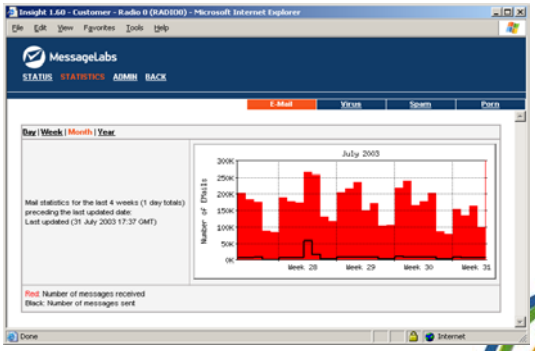
Virus Quarantine



Spam Statistics



Email Volume Statistics



Text Reports - Virus

TOTAL (All Domains):

Sent/Received	Number
Received	71
Sent	3

TOTAL (By Domain):

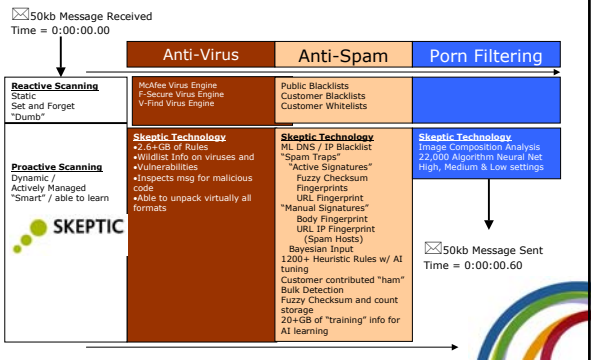
Sent/Received	Number
domain.com	
Received	67
Sent	3
domain2.com	
Received	4

SUMMARY By VirusType (All Domains)

Virus	Sent/Received	Number
Possible-virus	Received	22
W32/Sobig@MM	Received	22
W32/Klez.h@MM	Received	11
W32/Sobig.A@mm	Received	7
W32/Yaha.k@MM	Received	5
W32/Lentin.B@mm	Received	4
W32/Gauda.A@mm	Received	2
W32/Gauda@MM	Received	2
W32/Klez.E@mm	Received	2
is a joke program	Received	1
W32/Bugbear.A@mm	Received	1
W32/Bybeie.worm.B	Received	1
W32/Magistr.32768@mm	Received	1
W32/Klez.H@mm	Sent	3

SUMMARY By VirusType (By Domain)

Email Scanning Process



The Need for Proactive Protection

"…proactive systems that provide first-strike protection offer hope against all categories of Internet-based threats.

The idea behind the first-strike approach is to detect and prevent malicious code before it ever reaches the lab for analysis. We expect to see new proactive technologies emerge in the coming years, including behavior blocking, anomaly detection and new forms of heuristics. These systems will be crucial for protecting against fast-spreading threats . . .

[O]rganizations will have to . . . ensure both reactive and proactive protection."

Robert Clyde,VP and CTO Symantec Corporation
Exposing the Future of Internet Security
April 8, 2003

A Fully Managed Solution

Desktop Solutions:

- Require Frequent Updates
- Single Threat Focused
- Reactive Defense Model
- Ongoing Administration Needed
- No Reaction to Dynamic or Changing Threats

Gateway Solutions:

- Additional Hardware & Software Costs
- Additional Administration Resources
- Threats Already in Your Network
- Slow to React to Dynamic/Changing Threats

A Completely Managed Service:

- No Additional Hardware or Software Costs
- Minimal Administration Required
- Proactive Defense Against Dynamic/Changing Threats
- Complete Email Threat Protection
- No Threats Inside Your Network
- Quick Setup (Within 24 Hours)
- 24x7x365 "Follow the Sun" Customer Support

MessageLabs Differences

- Incoming and outgoing email scanning at the Internet Level
- 100% Virus Free Email (Known and Unknown)
- Fully redundant / globally load balanced network of 30 Control Towers
- Certified ISO 17799
- 7 Day Unlimited Volume Mail Bagging
- Absolute protection against Dictionary Attacks, Mail Bombs and DOS Attacks.
- No discernable latency (<1 sec)
- No hardware or software required
- World Class security staff watching over your business
- 24x7x365 Staffed Global Operations Center
- Effortless management interface via InSight

MessageLabs Service Overview

What Questions Can I Answer for You?

Contact
MessageLabs (Asia Pacific) Ltd
Level 14, 90 Arthur St, North Sydney, NSW, 2060
New York, NY 10018

www.messagelabs.com