



Spam and Malware Update: Industry Developments, Customer Pain Points

August 2007. Report excerpt #735

Ferris Research Analyzer Information Service

Ferris Research, Inc.
408 Columbus Ave., Suite 3A
San Francisco, Calif. 94133, USA
Phone: +1 (415) 986-1414
Fax: +1 (415) 986-5994
www.ferris.com

Recent Reports From Ferris Research

Email Sender Authentication
Four New Messaging Products and Services
Achieving Regulatory Compliance With Email and Internet Content Security Policy Enforcement
Key Messaging Issues: 2007 and Beyond
Meeting the Challenge of Email Discovery
Spam Control: The Current Landscape
Planning and Implementing an Email Archiving Solution
Instant Messaging: New Developments in Presence and Real Time Information Interchange
Identum's Private Post: Innovation in Email Encryption
Domino Unified Messaging Product Selection and Implementation Trends in Outbound Content Control
Reputation Services and Spam Control
Pushing the Limits on Exchange Storage
The Total Cost of Ownership for Voltage Identity-Based Encryption Solutions
Assessing and Managing the TCO of Mobile Messaging Devices
Email Archiving Technology Trends
Mobile Messaging for Exchange: Product Selection and Implementation Issues
Snapshot: Lucid8 GOexchange Preventive Maintenance
Microsoft's Latest Push for Notes and Domino Migration
Exchange Reliability and Its Impact on Organizations
Snapshot: Teneros—Application Continuity Appliance for Microsoft Exchange
Implementing Email Archiving
The Benefits of Integrating Enterprise Content Management Systems and Team Workspaces
Enterprise Mobile Messaging Survey
The Email Archiving Market, 2006-2010
Exchange 12 Assessment
Anti-Spam Technology in the Asia-Pacific Region
Why Exchange 12 Will Be 64-Bit Only
Top 10 Messaging & Collaboration Issues: 2006
The SyncML Standard and Its Impact on Mobile Messaging
Snapshot: Azaleos OneServer
Boundary Email Security: The First Line of Defense
Oracle Content Services: An Alternative to SharePoint Services for Enterprise Content Management
The Plan for AOL Instant Messaging

Table of Contents

Industry Developments	4
Reputation Services.....	4
Sender Authentication.....	4
Detecting Forgeries	4
SPF and Sender ID	5
Domain Keys Identified Mail.....	5
Which to Choose?	5
Enhancing Reputation Services.....	5
Domain Assurance Council	6
Vouch By Reference	6
Areas of Greatest Customer Pain	7
Spam Control	7
Effectiveness and False Negatives	7
False Positives	7
Productivity Issues With Quarantines	7
Quarantines Can Give Misleading Impression of Accuracy	8
Anti-Virus	8
Desktop Performance	8
Deliverability Problems	9
Performance and Scalability	9
Sponsorship of This Report.....	9

Industry Developments

Reputation Services

For several years, spam and virus control has been assisted by the use of DNS blacklists (DNSBLs). These lists cite rogue IP addresses and address ranges that have been observed sending spam, viruses, or other undesirable content. The lists are interrogated in real time, usually via a DNS query.

Some DNSBLs gained the reputation of being run by amateurs who carelessly blacklisted legitimate senders of bulk email. While not all DNSBLs are badly run, there have been several high-profile examples of DNSBL errors.

Several spam control vendors use a form of DNSBL, known as a *reputation service*. These vendors provide a professionally run service that rates the reputations—good, bad, or unknown—of IP addresses.

In the future, reputation services will identify senders by other means than just IP address. As we'll see in the next section, they will be able to track the reputation of sending domains as well. This is not possible today, as the purported sender of a message is too easy to forge, and such forgeries are difficult to detect.

Sender Authentication

Sender authentication, sometimes known as sender *authorization*, is a way of detecting forgeries. It allows domain owners to specify rules for recipients to determine whether or not an incoming message is from the purported sending domain.

Detecting Forgeries

Sender authentication is not, in and of itself, a spam control technique. However, it is useful for detecting forgeries, and so is increasingly employed as a defense against phishing.

Detecting phishing attacks via sender authentication depends on legitimate senders, such as PayPal, publishing information in the DNS. An email that purports to come from paypal.com can then be verified against that published information. (Of course, this doesn't stop phishers from using similar domains, such as verify-paypal.com.)

As more domains publish such information, recipients will be able to detect a larger proportion of forgeries.

SPF and Sender ID

The main sender authentication technologies used today are Sender Policy Framework (SPF), and its Microsoft-extended cousin, Sender ID Framework (SIDF). SPF and SIDF allow domain owners to publish a list of IP addresses that are authorized senders of email on behalf of the domain. The IP addresses are published in the DNS.

Thanks to some intellectual property squabbles within the Internet Engineering Task Force (IETF), these technologies failed to progress toward a formal standard. They are officially designated as experimental, although SPF is now essentially a de facto standard.

However, SPF and SIDF have limited usefulness. This is primarily because email that is automatically resent—such as via a mailing list or vanity domain—will usually break the recipient’s forgery detection algorithm. The problem happens when the message is resent but “sender” doesn’t change—a common occurrence. The original sender’s domain won’t match the resending MTA’s. There are ways around this problem, but they rely on the sender and/or the manager of the forwarder to install new versions of their MTAs.

Domain Keys Identified Mail

Domain Keys Identified Mail (DKIM) is a more complex technology that is less susceptible to the problems of SPF/SIDF. It relies on the sender signing the message at the boundary, using a public/private key pair. The public key is published in the DNS.

As you might expect, DKIM is more complex to set up, but it’s worth the extra effort because of the additional robustness.

At the time of writing, DKIM is on the path to becoming an IETF standard (i.e., an RFC, or Request for Comment). Draft 10 is being edited and is expected to be published before the middle of 2007.

Which to Choose?

It’s not a case of either SPF/SIDF *or* DKIM. The two technologies are complementary.

Ideally, sending domain owners should use both technologies, and receiving spam control solutions should have both in their suite of spam tests.

For more information on this and other aspects of sender authentication, please see Ferris Research report #713 *Email Sender Authentication* (May 2007).

Enhancing Reputation Services

Detecting forgeries isn’t the main use for sender authentication. As we noted in the previous section, reputation services can’t track the reputation of a sending domain unless the recipient can reliably detect a forged message sent in the name of that domain.

So, as the use of sender authentication becomes more widespread, reputation services will become more useful. In the future, they will be able to speak to the reputation of the sending domain, not just the particular IP address.

Domain Assurance Council

The Domain Assurance Council (DAC) is a trade body representing organizations that certify or accredit email sending organizations and customers of those organizations. Examples of such organizations include Habeas and Goodmail. Their customers are typically ISPs and spam control technology vendors.

With sender authentication becoming more popular, trusted authorities need a standard mechanism to vouch for a domain name. For example, a receiving mail system may be able to use SPF or DKIM to verify that an incoming message was sent by example.com, but it currently has no standard way of deciding if it wants to receive email from that company. The DAC plans to solve that problem by publishing reputation or accreditation data about a domain name in a standard form.

Vouch By Reference

The standard developed by DAC will be known as Vouch By Reference (VBR). Using VBR, a receiving system would be able to look up the domain and decide if it wishes to receive the message.

VBR could also allow organizations within vertical industries to vouch for other organizations in the same industry (e.g., the pharmaceutical industry). The theory is that organizations in vertical markets know each other so that if one is sending spam, then its competitors are likely the first to find out about it.

VBR will create a market for organizations that vouch for domains, allowing its members to compete with minimum friction. That's because VBR will also allow customers to switch providers—i.e., there will be no lock-in to a proprietary provider.

Areas of Greatest Customer Pain

Most of the current email defensive technologies today have some drawbacks. Following are the key areas where IT departments and the majority of end users experience the greatest difficulties, together with an indication of whether these problems have been getting worse over the past six months.

Spam Control

Maintaining spam filtering accuracy seems to be a constant struggle for many customers and their spam control vendors. For some vendors, it's a struggle they're losing.

Effectiveness and False Negatives

The effectiveness of many spam filters has been falling. The most visible accuracy failures are false negatives—spam that makes it through to the inbox. As we discussed earlier, many false negatives are the result of new techniques, such as morphing images.

False Positives

However, there's an even more insidious accuracy problem: false positives. This refers to legitimate email that's accidentally filtered as spam. The productivity impact of a single false positive can wipe out the productivity gains made by filtering hundreds of spam messages.

Some vendors that are experiencing falling effectiveness try to fix the problem by increasing the aggressiveness of their filters. However, this typically causes more legitimate email to be caught in the same net. As noted earlier, another key cause of false positives is overly aggressive blacklisting. False positives are particularly prevalent with legitimate bulk email, such as newsletters.

While the general trend is for false positives to decrease, the less competent spam filters are causing more false positives recently.

Productivity Issues with Quarantines

Many spam filters will put incoming spam in a “spam folder,” or quarantine. Users can check these quarantines for legitimate email. Unfortunately, few users regularly do this.

Also, checking the quarantine can waste the productivity benefits gained by filtering spam. This problem has gotten worse as spam levels have risen.

Furthermore, quarantines do not block unsolicited pornography, so that users may be forced to view pornographic emails during the course of checking the quarantine.

For these reasons, the best spam control technologies only quarantine the absolute minimum of messages—those that the technology *thinks* are spam, but isn't positive about. However, when the spam control system is certain that a message is spam, the message is deleted, so the user doesn't see it in the quarantine. Such a restricted quarantine doesn't waste as much employee time and is more likely to shield users from obscene emails.

The best vendors also provide users with effective, efficient tools for searching the quarantine.

Quarantines Can Give Misleading Impression of Accuracy

A restricted quarantine can give the more naïve user the misleading impression that the quarantine contains all of the spam received, minus those few that made it into the inbox. That, in turn, can lead users to think the spam filter isn't very accurate.

For example, if a user receives 400 spam messages in a week, but only 50 of them are admitted to the quarantine, and 10 more slip through to the inbox, the actual effectiveness of the filter is 98%. But if the user isn't aware of the 340 blocked messages, then he or she would assume that the spam filtering effectiveness was only 83%. The last thing that IT wants to hear is grumbling based on incorrect statistics. One solution for IT is to regularly publish its spam blocking stats.

Anti-Virus

As we discussed earlier, email remains a key vector for the spread of viruses, worms, Trojans, and other malware. Traditional signature-based AV products and services continue to be the main way that organizations can protect themselves from infection.

To provide reasonable coverage against threats, organizations should implement AV on at least two levels: at the network boundary and at the desktop. The AV on each level should inspect the files and network behavior of all applications, including email, Web access, and instant messaging.

Desktop Performance

Some vendors' desktop AV products have substantially grown in functionality and footprint. This software "bloat" can levy a penalty in performance.

Organizations should ensure that their chosen desktop AV technology doesn't impose such a performance penalty that users are tempted to disable it, or switch off functionality such as scan-on-access or heuristic scanning.

Deliverability Problems

Deliverability generally refers to the level of success an email marketer has in getting email delivered to the inbox. However, regular email users are also concerned with deliverability. If an IP address used for outgoing email of an organization or ISP gets blacklisted, it's much less likely that the organization's email will be delivered.

This can happen for several reasons, including:

- The organization is unwittingly hosting zombies that send spam.
- It has thoughtless or naïve marketers who resort to sending spam.
- It shares an IP address or IP range with a spammer.

Performance and Scalability

As spam volumes rise and anti-spam technologies get more complex, organizations will experience delayed incoming email. This is usually the result of too much email clogging the spam filter and slowing performance.

As the peak inbound email demand (usually expressed as numbers of messages per minute) reaches a critical point, overloaded MTAs begin to drop connections. This causes email to be queued for redelivery. At best, this means delays of minutes or hours. At worst, continued failed delivery attempts will cause email to bounce back to the sender with a nondelivery report.

Organizations must ensure that their chosen spam control technologies can handle the expected volume of email, including accounting for the increases in demand over its lifetime. This means that the technology is able to accept, filter, and pass on messages with minimal delay.

*Author: Richi Jennings
Editor: Sue Hildreth*

Sponsorship of This Report

This report was sponsored by [SonicWALL](#), which has the right to distribute copies of it in electronic format. Ferris Research independently conducted all research and retained full editorial control. You may copy or freely reproduce this document provided you disclose authorship and sponsorship and include this notice.

About SonicWALL

SonicWALL designs, develops, and manufactures solutions that provide network and data protection, including network security, secure remote access, Web and email security, and backup and recovery. The company helps organizations of all sizes protect their networks and sensitive information. With appliance-based solutions and subscription services, SonicWALL's portfolio of solutions delivers enterprise-class Internet and data protection.

Ferris Research

Ferris Research is a market research firm specializing in messaging and collaborative technologies. We provide business, market, and technical intelligence to vendors and corporate IT managers worldwide with analysts located in North America, Europe, and the Asia-Pacific region.

To help clients track the technology and spot important developments, Ferris publishes reports, white papers, bulletins, and a news wire; organizes conferences and surveys; and provides customized consulting. In business since 1991, we enjoy an international reputation as the leading firm in our field, and have by far the largest and most experienced research team covering messaging and collaboration.

Ferris Research is located at 408 Columbus Ave., Suite 3A, San Francisco, Calif. 94133, USA. For more information, visit www.ferris.com or call +1 (415) 986-1414.

Spam and Other Email Threats: Market and Technology Update

Readers seeking further discussion of recent malware control developments may wish to read *Spam and Other Email Threats: Market and Technology Update*, published by Ferris Research. Additional topics include:

- Recent spam threats—including stock kiting gangs, new spammer techniques, and new botnet threats—and their implications.
- Viruses by email.
- Phishing.
- Nigerian 419, fake lottery and other types of advance-fee fraud.
- Buyers' evolving purchasing requirements for malware control.
- Buyers' sources of information.

For more information, visit <http://www.ferris.com/2007/06/08/spam-and-other-email-threats-market-and-technology-update/>.

Free News Service

Ferris Research publishes a free daily news service. It provides comprehensive coverage of the messaging and collaboration field, and is a great way to keep current. Topics include spam, email, email retention/archiving, mobile messaging devices, consumer messaging services, Web conferencing, email encryption, email migrations and upgrades, regulations compliance, instant messaging, ISP messaging, and team workspaces.

The news is distributed daily. To register, go to <http://www.ferris.com/services/free-news-service/>. In addition, you will receive one or two emails every month announcing new Ferris reports or conferences. To opt out and suppress further email from Ferris Research, click on the opt-out button at the end of each news mailing.