The Impact of Messaging and Web Threats

An Osterman Research White Paper

Published April 2008

SPONSORED BY

Sunbelt Software

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Messaging Security is Becoming More Difficult

THE IMPORTANCE OF ELECTRONIC COMMUNICATION

Email is the most critical communication tool in the workplace, as evidenced by these results from a February 2008 report published by Osterman Research:

- The average user in an organization of up to 1,000 employees sends and receives 124 emails on a typical workday; the average user in a larger organization sends and receives 149 emails each day.
- Considering all of the communication that employees send during a typical day – email, letters, instant messages, blog posts, wiki postings, etc. – email accounts for 74% of the total volume of content sent.
- 58% of email users report that email is critical in helping them to get their work done, while another 35% believe that email is important.

> Because 58% find email to be critical in getting their work done, and because other communication tools are becoming more widely used, attacks directed against these capabilities threaten the very ability of individuals and companies to communicate or protect their sensitive data.

Because email is so critical, and because other communication tools – instant messaging, wikis, blogs, VoIP, collaboration tools and other capabilities – are becoming more widely used, attacks directed against these channels threaten the very ability of individuals and companies to communicate or protect their sensitive data.

SPAMMERS AND HACKERS ARE MOTIVATED BY PROFIT

While early spammers, virus developers and hackers were motivated primarily by notoriety and the challenge of spreading their wares; modern-day attacks are motivated mostly by profit. Spammers, for example, can earn significant amounts of money by selling products marketed through spam – such as stock "pump-and-dump" schemes – or by directing people to advertising-laden sites on which they earn a commission for clickthroughs. Virus writers, phishers, developers of keystroke loggers and others can make money by stealing it from bank accounts or via fraudulent credit card transactions; or they can simply sell this account information to others.

The profit motive has dramatically exacerbated the threats faced by messaging and Web users. Because significant profits are available to spammers, phishers, criminal networks and others, many people have been attracted to this "market". Further, because profits from malicious activities are substantial, they can be used to fund newer and better methods for circumventing defenses against their attacks.

BOTNETS ARE A CRITICAL PROBLEM

In the past, spammers sent large numbers of messages from a small number of sources that were fairly easy to identify and block. More recently, however, spammers have created botnets that consist of millions of 'zombie' computers – computers in homes and the workplace that are infected with a virus, worm or Trojan that permits them to be controlled by a remote entity. According to Commtouch, more than 85% of spam messages and nearly 100% of malware messages are sent from zombie machines. As of early 2008, Google Message Security had tracked a 62% increase in the daily number of unique IP addresses that are blocked by its network compared to early 2007. This is a clear indication of the growth of botnets.

Spammers can rent botnets for content-distribution campaigns. Using botnets, a small number of messages can be sent from each of thousands of computers, effectively hiding each zombie from detection by ISPs or network administrators using conventional tools. Botnets are a critical problem not only because they are responsible for the vast majority of spam sent across the Internet today, but also because they are used for a wide range of purposes beyond just spam delivery. These include hosting malware sites, perpetrating distributed denial-of-service attacks, click fraud and credit card fraud. Botnets can be hard to detect and hard to remove.

WEB-BASED THREATS ARE A SERIOUS PROBLEM, AS WELL

There has been a huge increase in malicious Web-borne content, including email messages that contain links to dangerous Web sites, attachments that are little more than stage-one downloaders of other malicious code from the Web, malware that installs and opens a communication channel to the attacking source, and other exploits. Typically, these malware sites succeed in creating more zombie bots that keep feeding the vicious cycle of spam and viruses.

Spam and Web-based threats are being used together increasingly in coordinated attacks. For example, Google has identified more than three million unique URLs on more than 180,000 Web sites that automatically install malware on visitors' machines – spam often is used to drive traffic to these sites simply for the purpose of installing malware for later use.

Further, Web 2.0 Web sites that include dynamic content, such as complex mashups that change continually, make it difficult to accurately determine whether a particular site is safe or risky at any point in time. This makes the need for real-time assessments and reputation more critical than ever before.

OTHER TECHNIQUES ABOUND

Among the techniques that spammers, phishers and others use to distribute their attacks are:

- **Spam filter-avoidance techniques**
  The simpler of these techniques involves text obfuscation, such as misspelling keywords; Bayesian poisoning (the process of including specific keywords into spam messages in an attempt to trick Bayesian filters into thinking a message is legitimate); introducing valid text into spam messages; using various HTML techniques to fool

filters into not recognizing offensive content; and other techniques. These techniques typically can bypass many traditional content-filters, and those using a Bayesian approach.

- **Newer types of spam**
  Starting in earnest in early 2006, spammers began using newer spamming techniques in an effort to defeat spam-filtering technologies. For example:

  - **Image-based spam**
    Text is represented as one or more images that typically use non-standard fonts, background 'snow', randomized backgrounds, slanted lines of text, blurriness and other distortions to defeat more conventional spam-filtering technologies, as shown in the example at right. Image spam is a particularly serious problem for mail servers and recipients, since each message is typically much larger than a conventional, text-based spam message. Image spam, while still used by spammers, is less of a problem today than it was in 2007.

  - **Spam with attachments**
    Similar to image spam, but using PDF files, spreadsheets or ZIP files as payloads to carry the spam content. An even newer technique is to send calendar invitations as malicious email attachments.

  - **Alternative spam languages**
    Spammers will often target their content to users who speak specific languages. There is a growing trend for more localized distribution with diversified languages.

  - **Audio spam**
    In October 2007, the first MP3 spam was found on the Internet advertising a stock "pump-and-dump" scheme. These audio messages, recorded at a relatively low bit rate, typically run for less than one minute and tend to be much larger than conventional, text-based spam.

- **Modular Trojans**
  This form of attack, also known as multi-stage downloaders, operate on a simple principle: a small Trojan first disables local anti-virus software or other security defenses. Once those tools are disabled, a second-stage of the attack downloads any of a variety of threats, including keystroke loggers, worms or other software typically designed to take control of the platform. Attackers who successfully disable anti-virus defenses are free to download virtually any sort of malware, including old viruses and

other threats, since these will no longer be detected.

- **Serial variants / server-side polymorphic malware**
  An effective attack technique is to create a series of variants of a single threat, each of which has been prepared prior to the introduction of the first variant. Each variant is launched at pre-determined intervals and is able to take advantage of networks' lack of signatures to deal with each new instance of the attack. For example, if each variant were launched at intervals of 12 hours, 100 variants of the same attack would leave open a 50-day window of vulnerability.

- **Phishing**
  Phishing is becoming more targeted, spoofing businesses that have smaller customer bases (e.g., local banks) to increase the effectiveness of the social engineering tricks used. Phishing will also continue to expand beyond online banks to include more retailers, online gaming and other online sources that process confidential account information.

Phishing is becoming more targeted, spoofing businesses that have smaller customer bases to increase the effectiveness of the social engineering tricks used.

- **Instant messaging threats**
  Instant messaging exploits, which often are blended threats, take the form of either "social engineering" techniques that will direct victims to an infected Web site; or via viruses, spyware or other malicious content that are delivered directly to the instant messaging client via a downloaded file. Instant messaging threats are particularly insidious, since the opt-in nature of instant messaging contact lists motivates recipients to trust that messages they receive are from valid senders whom they have previously authorized to send them content.

- **Combination, or blended threats**
  Combination threats are payloads that mix several delivery modes (such as email and Web) and often contain multiple components, such as:

  - Spam
  - Phishing
  - Viruses
  - Worms
  - Trojans

  Further, these threats can combine protocols, such as emails that link to malicious Web sites.

- **Social engineering**
  Increasingly sophisticated techniques are being employed to trick users into thinking an email and the associated links are legitimate. Whereas spam aiming to sell a

product is relatively easy to spot, spam containing security threats from phishing, viruses, spyware, and other malware is difficult to detect when obscured in this manner. This is a particularly serious problem for instant messaging-borne threats, as noted above, since instant messaging systems are inherently more "trustworthy" because recipients of these communications must first allow individuals to send them content. If someone receives a worm-generated instant message, there is a much greater likelihood that the recipient will assume the message is valid and open it without hesitation.

In general, threats are becoming more regionalized, more targeted to specific organizations and groups, and more difficult to thwart. The entire malware "industry" is becoming more sophisticated, driven increasingly by criminal networks and a greater emphasis on traditional business models. For example, spammers can purchase lists of fresh email addresses, rent a botnet for distribution of their content that will provide service-level guarantees, and achieve measurable rates of return on their investments. In short, the problems associated with malware are becoming much worse.

What are the Risks and Costs of These Attacks?

There are a variety of problems caused by the threats discussed above:

- **Business risks**
  The security risks from spam are very real – they are no longer just a nuisance. The growing variety of keystroke loggers, password-stealing Trojans and other threats means that corporate data is increasingly at risk. Data theft can include sensitive content like usernames and passwords, but also financial data, customer data, trade secrets and other types of confidential information. The increasing end goals of stealing information (personal and corporate), hijacking systems for a wide range of purposes and launching additional malicious attacks all have serious business implications, in addition to the more traditional (but still real) impacts to bandwidth, infrastructure and other costs.

- **Bandwidth constraints**
  Spam and other malicious content that enters the corporate network consumes network bandwidth that could otherwise be used for legitimate purposes. As the volume and file size of this content increases, bandwidth is consumed for non-legitimate purposes, in many cases requiring the deployment of larger data pipes at greater cost simply to maintain acceptable system performance, message delivery times, Web access times and the like.

- **Storage requirements**
  As more malicious content comes into a network, more of this content must be stored for review in quarantines and archives. Given that this content is normally preserved for at least 30 days in order to give employees time to review it for false positives, increases in malicious content entering a network inevitably lead to increased storage requirements. Further, storage spikes add significant volatility to storage needs, making

it difficult to plan storage capacity accurately.

For companies with strict data retention policies that need to maintain a reliable record of communication for compliance purposes or because of anticipated litigation requirements, even quarantined data may need to be stored for several years, further bloating storage requirements. Many organizations also store all email accepted by the messaging infrastructure based on the company's email use policy, as well as e-discovery and other legal requirements.

- **Loss of productivity**
  While some believe that spam causes a major loss of *employee* productivity, Osterman Research has found that this is actually a real, but relatively minor, problem in the overall context of the spam problem, particularly for organizations that have robust spam-filtering defenses. That said, Web-borne threats or attacks that reach end users via email can cause very serious problems, including employee identity theft, loss of data or damage to computer hardware.

  However, malware can cause significant losses of *IT* productivity, since IT staff members must often spend extra time remediating problems caused by malware, more FTE staff must be available to address unforeseen problems, etc.

- **Other problems**
  There are a variety of other problems related to malicious content, including some employees spending time perusing products and services offered in spam, links contained in messages that could direct users to harmful or offensive Web sites, and other problems.

OUTBOUND CHALLENGES

Electronic communication carries with it the substantial risk that employees might communicate in ways that violate corporate policies, various statutes or best practices. For example, the ease with which an email or instant message can be sent means that trade secrets or other sensitive information can be sent in ways that are contrary to the best interests of an organization. While most data breaches are unintentional – employees will often send confidential data inadvertently – there are some employees that may intentionally violate corporate data confidentiality policies.

Hosted services are increasing in popularity and offer another option for organizations to implement a variety of threat-protection capabilities.

An Osterman Research survey found that if a data breach were to occur in which disclosure of the breach would have to be made to customers and other external contacts, nearly two-thirds of organizations estimated that a single breach would cost their organization at least $100,000, as well as other operational costs, damage to their brand and other problems.

For the most part, organizations have almost universally deployed systems that protect against inbound threats, such as viruses, worms and spam. Far fewer organizations have deployed systems that monitor outbound content. However, the growing use of email and instant messaging, coupled with the growing variety of other communication tools available to employees, makes the monitoring and management of outbound content increasingly important. This means that organizations must focus on data leakage protection (DLP), coupled with automatic encryption of sensitive content to protect themselves from a wide variety of data breaches.

Another outbound threat is the danger that the organization itself may become a source of spam or malware, due to infection, or even malicious behavior by an authorized user. Besides wasting the IT resources of the organization, becoming a spam or malware source has other, more damaging effects: it can harm the organization's profitability due to blocked legitimate communication or breaches in mission-critical systems, and it can expose the organization to potential litigation due to damage it caused by unwittingly being a source of spam or malware.

Considering Delivery Models

There are a variety of ways in which messaging and Web security capabilities can be managed, including:

Gateway-Based Systems
Gateway security stops threats at the earliest possible point in the on-premise mail infrastructure and is a best practice for organizations that manage on-premise defenses.

Server-Based Systems
On-premise solutions deployed at the server level resolve many of the problems associated with client-side systems by allowing easier deployment and management capabilities, as well as the ability to more easily enforce corporate policies and changes through a centralized management interface. Mail server security centrally protects internal email, incoming email (e.g., POP3 email forwarded to Outlook) that bypasses the gateway and the mail store.

Client-Based Systems
Client-based systems, such as URL filtering tools, anti-virus tools, spyware blockers and the like provide useful capabilities and can be very effective at preventing a variety of threats – client-side anti-virus tools, for example, are an important best practice for any organization.

Client-side capabilities can be relatively inexpensive and are often provided as part of desktop protection suites that include anti-virus, anti-spam and other capabilities. While client-side systems are effective in smaller organizations, they often do not scale well. They are time-consuming to install and update for large numbers of users and can be quite expensive to deploy in larger organizations. Particularly for larger organizations,

centralized management and deployment capabilities are essential to cost-effectively install, update and enforce corporate policies using client-based systems.

SaaS and Hosted Services

SaaS and hosted services are increasing in popularity and offer another option for organizations to implement a variety of threat-protection capabilities. The primary advantages of this model are that no investments in infrastructure are required, up-front costs are minimal, ongoing costs are predictable, and all management and upgrades of the system are provided by the SaaS or hosted service.

The disadvantage of SaaS or hosted services is that their costs *can* be higher than for on-premise systems in some situations, although they will not *necessarily* be more expensive. For example, SaaS vendors merely rent space on a server, providing a very inexpensive method for accessing software and infrastructure technologies. Although organizations may pay more to a SaaS or hosted security vendor than they would for an on-site solution, the value of the hosted infrastructure and administration provided by the third party vendor can provide a lower Total Cost of Ownership.

SaaS vendors merely rent space on a server, providing a very inexpensive method for accessing software and infrastructure technologies.

Managed Services

Managed services are similar in concept to hosted services, but a third party – either with staff on-site or via a remote service – manages the on-premise infrastructure, installs upgrades, updates signature files and the like. Costs can vary widely for managed services depending on the size of the organization, whether third-party management personnel are located on-premise or in the third party's data center, and other factors.

Hybrid Offerings

A newer approach that is increasingly offered by vendors is to combine on-premise infrastructure with hosted services. For example, a vendor may provide a spam-filtering appliance on-site, but couple this with a hosted spam-filtering service that acts as a sort of pre-filter; or they may rely on a hosted anti-virus service and desktop anti-virus tools.

The fundamental advantage of this approach is that the on-premise infrastructure is protected from spikes and overall increases in the volume of malicious traffic over time, thereby preserving the on-premise investment and maintaining acceptable performance of their messaging and Web infrastructure.

New Approaches Are Needed

MULTIPLE LAYERS OF DEFENSE ARE REQUIRED

The most effective approach to dealing with spam, viruses, Trojans, worms and other forms of malware is to employ a layered defensive strategy that will deal with all threats at a variety of venues. Furthermore, to be truly effective against today's sophisticated attacks, each layer must provide an integrated defense against multiple types of attacks.

- **Perimeter defense** that blocks connections based on the email sender's reputation can eliminate the majority of malicious email traffic before it ever enters the organization's network. A real-time dynamic reputation service that identifies zombie botnets as they are activated will significantly reduce these rogue computers' threat.

  Gateway technologies, such as reputation services, are critical to blocking the bulk of email threats before they even enter the network and will preserve bandwidth and reduce storage requirements for quarantines and archives. Other technologies can block threats at the gateway before they penetrate the network and negatively impact the messaging infrastructure.

- **Servers** are also a critical venue on which appropriate defenses must be installed, effectively creating a robust defense for threats that make it past the gateway. These defenses include systems to inspect for and detect viruses, worms, Trojans, intrusion attempts and other email and Web-borne threats. The mail server can provide another layer of threat protection and is the only central point that will catch internal emails harboring threats. Also, as the only location that filters interoffice as well as outbound email, the mail server is the most effective point at which to deploy DLP and compliance filtering for messaging.

> Just as multiple physical layers of defense are required, multiple threat-detection and remediation techniques are also needed.

- **Outgoing content inspection/DLP** is becoming increasingly important to prevent the leakage of sensitive data, typically by users who inadvertently send this content through email, instant messaging systems, Webmail, wikis, blogs, etc. These systems can protect an organization from intentional attempts to circumvent corporate policies and the much more common inadvertent transmission of sensitive data. It is critical to couple DLP with encryption to ensure that sensitive data is encrypted automatically before it is sent outside the organization. Outbound detection can also prevent the organization from becoming a source for spam or malware.

- **Client-side systems** are critical to deal with malware that may be introduced by users bringing in files on USB thumb drives, files that might be downloaded to corporate servers from a home computer, etc. Client-side systems must be installed wherever threats might be introduced: on desktop systems, laptops, mobile devices, home computers, etc.

More serious implications on the client side (and also on servers), however, are caused by the growth of Web-based applications. Because more capabilities are being introduced into the client-side experience, code is being executed within a Web browser more often than used to be the case in the days of early Web sites and applications. This creates more opportunities for hackers and others to negatively impact users and the networks on which they operate in a variety of ways.

MULTIPLE TECHNIQUES ARE REQUIRED

Just as multiple physical layers of defense are required, multiple threat-detection and remediation techniques are also an important best practice. These include

- Traditional content-inspection and pattern-detection systems, as in the case of spam filtering.
- Signature-based systems to look for spam, viruses, worms, Trojans and the like.
- Zero-day and zero-hour protection systems that can block or quarantine suspect content that has not previously been detected.
- Reputation and connection management systems that will inspect further back in the traffic stream and prevent the delivery of suspect content or content from non-credible sources.
- A variety of "in-the-cloud" services that will provide detection and remediation capabilities before content ever reaches a corporate network.

IDENTIFYING THE SOURCE IS BEST

While identifying and blocking spam and other malware at its destination is good, stopping this unwanted content as far back in the delivery chain is significantly better. By identifying zombies and other sources of malware before their content has been delivered, an organization can dramatically reduce the amount of CPU capacity, storage and bandwidth necessary to process unwanted content. This means that organizations should use reputation analysis and connection management systems where appropriate to block or throttle content from suspect sources.

The Future of Messaging and Web Threats

Osterman Research anticipates these trends in the messaging threat landscape:

- Continuing growth of spam, sent primarily by growing numbers of zombie computers in botnets. While there are many entities that attempt to combat the growth of botnets, user behavior and lax security procedures – particularly by home users – will ensure that malicious code will find a platform from which to operate.
- Increasing attacks against mobile devices will also be a key threat in 2008 and beyond as the number of mobile devices grows and as mobile-specific applications are

developed to make these devices more useful in a business context. The success of the Apple iPhone, for example, will attract a growing number of hackers.

- Increasing attacks on social networking sites in which users' pages on these sites will have malware installed in order to infect visitors to these pages. The threat is particularly problematic because social networking sites are so popular. For example, according to comScore, in December 2007 MySpace had 38.3 million page views and Facebook had 13.0 million page views, to name but two of the many popular social networking sites in use.

- Legitimate Web sites will also be targeted. For example, a number of legitimate Web sites have already been hacked to host malware or to redirect visitors to malware sites, including the German version of Wikipedia in late 2006, the Asus Web site in April 2007, the Monster.com Web site in August 2007, and the Web site for the UK's Forth Road Bridge in February 2008.

- Increasing numbers of dynamic exploits, whereby threats are modified on the fly in an attempt to defeat signature-based defense mechanisms. These polymorphic viruses, worms and other exploits can defeat some anti-virus defenses.

DLP systems, coupled with policy-based encryption, will become more widely deployed as decision makers realize their need to protect the confidentiality of corporate data.

- Growing numbers of instant messaging and other real-time threats. For example, FaceTime reported its discovery of 1,088 threats during 2007 directed against instant messaging, chat and peer-to-peer file sharing systems. Further, the company found that IRC-focused attacks are on the increase.

- Attacks directed against Internet telephony systems will become more common. Although dating back to 2005, IP telephony threats were somewhat more common during 2007 and will be increasingly common in 2008 and beyond. For example, Finjan discovered three separate Spam over Internet Telephony (SPIT) attacks during 2007. Attacks against Skype users will become more common.

- DLP systems, coupled with policy-based encryption, will become more widely deployed as organizational decision makers realize their need to protect the confidentiality of corporate data in response to data leaks, statutory requirements and other motivators.

- There will be increased numbers of URLs delivered via email that take recipients to malicious websites.

- There will be more regionalized attacks using local languages and more targeted attack methods.

Sunbelt Software's Approach for Addressing Security

Sunbelt Software has been delivering best-of-breed, award-winning server-based email security software for years. For Exchange environments, Sunbelt's Ninja Email Security offers an advanced and powerful, policy-based email security product that provides a layered security approach for email inspection, cleansing and management. By using multiple scanning engines for anti-spam and antivirus, and integrating powerful custom rules, all treatment of messages occurs at the server, not at end-users' workstations – no client software is needed.

Summary

Messaging, internal and Web-based threats are increasing in number and severity. Because the profit motive now drives spammers, hackers and other purveyors of malicious content, as well as the development of more sophisticated techniques to circumvent corporate defenses, organizations must continue to improve their defenses. Plus, organizations must protect against internal users from sending confidential content out of the organization through a variety of communication tools, whether this activity is intentional or accidental.

The risks to organizations large and small are not theoretical – there are real problems that users and their employers face if they do not establish adequate defenses against the growing variety of malware, exploits and other threats that are directed against them.

Organizations must deploy defenses at all of the physical venues at which threats may enter a network or through which users may intentionally or inadvertently send sensitive content; and they must implement a layered defensive strategy to protect against all types of threats.

Sponsor of this White Paper

Headquartered in Tampa Bay (Clearwater), Florida, Sunbelt Software was founded in 1994 and is a leading provider of Windows security and management software with product solutions in the areas of anti-spam and antivirus, antispyware, and vulnerability assessment. Leading products include the CounterSpy product line, Ninja Email Security, Sunbelt Exchange Archiver, and endpoint firewall technologies.

Sunbelt Software
33 North Garden Avenue
Suite 1200
Clearwater, FL 33755
+1 888 688 8457
www.sunbeltsoftware.com

For email security Sunbelt offers an award-winning solution for combating spam, viruses, and other email threats for complete protection for the messaging infrastructure. Ninja Email Security is an advanced and powerful, policy-based email security product for Microsoft Exchange that provides system administrators the weapon to enforce email policies that protect their network against spam, phishing, viruses and other messaging security threats. Ninja provides a layered security approach for email inspection, cleansing and management. By using multiple scanning engines for anti-spam and anti-virus, while integrating other email security rules, all treatment of messages occurs at the server, not at your end-users' workstations – no client software needed.