

WHITE PAPER

CommTouch Reputation Service: Fighting in the Gray Zone

Sponsored by: CommTouch

January 2007

IDC OPINION

The problem of spam and other unwanted email has reached epidemic proportions making it increasingly hard to control. Although existing solutions can still block most email-borne threats, the use of sophisticated techniques to avoid detection by content filters, as well as the increasing use of botnets and zombie machines, have made it easier for malware writers to circumvent security systems. This surge in unwanted email places a significant burden on organizations, particularly in terms of the misuse of email resources, loss of employee productivity, and reduced network performance. This situation highlights the need to block unwanted email before it enters the corporate network. One approach deemed effective as such a first line of defense is reputation filtering, which is based on analyzing the behavior of the sender's IP address and other factors to determine whether it is a source of malware or spam. Traditionally, reputation filters maintained blacklists of IP addresses known to be sources of spam or other malware and blocked all email traffic from these IPs. But as millions of zombie machines are being hijacked on a daily basis across the world, the number of "gray" IP addresses about which no previous information is available is on the rise. As a result, traditional reputation filters are struggling with growing numbers of IP addresses that cannot be classified as either "good" or "bad".

Given current malware trends, demand for reputation filtering solutions to complement traditional messaging security is on the rise. But for reputation filtering to be effective against emerging threats, and against zombies and gray IPs in particular, it needs to evolve to include capabilities such as real-time classification and global threat coverage.

METHODOLOGY

IDC developed this white paper using a combination of existing market forecasts and direct, in-depth, primary research. To gain insight into the challenges posed by modern spam and other types of malware, and to learn about how CommTouch's Reputation Service can help mitigate those risks, IDC interviewed the company team on the issues of technology, product offerings, competitive landscape, and go-to-market strategy. IDC also interviewed companies employing CommTouch's technology, including Sendmail and Telepak.

IN THIS WHITE PAPER

This IDC white paper looks at the problem of modern email-borne malware, which is becoming increasingly evasive to traditional messaging security solutions. It illustrates the need for content-agnostic solutions that analyze the behavior of the sender's IP address in order to stop spam and other threats at the network perimeter, thus reducing the burden on IT resources. The paper provides an overview of traditional

reputation filtering approaches and their weaknesses, and how new approaches can be utilized to tackle challenging threats such as zombie machines and botnets used by hackers and criminals for launching financially-motivated attacks.

SITUATION OVERVIEW

Current Malware Trends

The "arms race" between malware writers and the security industry continues to evolve, as attacks become increasingly complex and sophisticated. It is a "Wild, Wild Web" out there today, with countless number of worms, viruses, Trojan horses, spam, spyware, adware, phishing scams, and other types of malware lurking in every corner. Although IT security is constantly evolving to keep pace, emerging threats still pose significant challenges.

To a large extent, the dramatic rise in the complexity and efficiency of attacks is a result of the increasing involvement of sophisticated hackers and organized crime groups motivated by financial gain. Correspondingly, a growing number of attacks revolve around fraud, identity theft, data theft, and other forms of financial motivation – these are also known as crimeware. It is no longer the sole territory of computer geeks and script kiddies writing viruses and worms to wreak havoc and gain infamy.

The footprints of sophisticated professionals can easily be observed in today's malware attacks, which are often designed to exploit the weak spots of traditional security solutions. For example, many of today's attacks that employ zombie propagation methods to spread spyware, Trojan horses, and other malware are based on sending hundreds of millions of messages within a few hours, completing a distribution cycle before antispam and antivirus signatures can be made available to users. Multi-variant viruses are another example of sophisticated attacks: malware writers prepare an "arsenal" of virus variants, each of which cannot be blocked using the same signature, released in time intervals to avoid interception by virus signatures.

Another indication of the growing sophistication of malware attacks is the increasing popularity of blended threats, which combine the characteristics of several malware types, including spam, viruses, worms, and Trojan horses, among others. Most blended attacks are designed to exploit known vulnerabilities in order to spread through multiple channels (e.g., email, Web).

Spam: Much More Than Just a Nuisance

Despite the massive deployment of antispam solutions, spammers continuously find new ways to challenge traditional defenses. A current example is image-based spam, which is increasingly being used to evade spam content filters by including only images with no text or hyperlink attached. An image-based spam message may appear to be text but in fact it just an image of text. In some cases, an image-based spam message will include text taken from legitimate books to elude Bayesian filters. Some antispam solutions have adapted to this threat by analyzing the image data itself. But spammers have responded by slightly changing image attributes (e.g., background, border shade, line spacing) for each message in a random manner to make it harder to identify an attack and develop corresponding signatures.

According to Commtouch, the volume of image-based spam grew substantially throughout 2006, reaching 50% of all spam at its peak distribution. Some recent attacks introduced new techniques that make it even harder for spam filters to catch and block them. For example, some attacks used animated images that comprise several frames played repeatedly. The main spam message is included in one of those frames while the other frames contain plain or random content. Another recently introduced technique is splitting a single image into smaller pieces; in other cases a “patchwork” approach with wavy text is used to fool OCR-based filters.

The rising volumes of image-based spam places a significant burden on organizations' bandwidth resources, as the typical size of an image spam is five to eight times (in the case of animated image spam) larger than text-based spam, which weighs 5.5KB on average. According to Commtouch, image-based spam now accounts for 35% of all spam on average (compared to less than 10% in 2005), which brings the total bandwidth and storage consumption of spam messages to new heights. In this regard, it is important to note that although antispam solutions are improving their accuracy and ability to block the vast majority of spam that penetrates corporate boundaries, dealing with the huge amount of spam messages still requires significant mail server resources.

FIGURE 1

Two Messages from the Same Image-Based Spam Attack

From: Tom Lopez [mailto:tom@047media.com]
 To:
 Cc:
 Subject: random

Wondering what's the top thing you need as a trader? The answer is confidence. Trading is about confidence, and you can't get it without reliable market information!
 Now listen. This stock could help you make huge amounts of money in weeks!
The alert is ON!

Get EGLY First Thing THURSDAY!
 This Is Going To Explode!
 Check out for HOT NEWS!

Thursday, August 3, 2006
Ever-Glory International Group, Inc (EGLY.OB)
CURRENT PRICE: \$0.99
GET IT NOW!

Ride on the big wave of opportunity presented by this stock.

Do you know the greatest thing about money? It allows you not to do things you dislike! So, I wish you to make enough money to get this opportunity!

Will my father, the Sheikh Hoster, do this? And with this Elnak was perfect content. How is it, Kinnak, a woEY? The Sorcerer glanced after it, a wrinkled smile spreading on his aged face. It was the year after that and Nonsak as well were unconscious, a shapeless, tumbled mound in the half-light. Here was a great this last in a sort of beavard, when, in a flash, the great idea came to him. But Kinnak saw that the odds drifted off into a sort of blind wonder at what it all meant. But if indeed she does not like me, why then do

From: Ellen Welsh [mailto:elw@blackboardinc.com]
 To:
 Cc:
 Subject: mine selling point

Wondering what's the top thing you need as a trader? The answer is confidence. Trading is about confidence, and you can't get it without reliable market information!
 Now listen. This stock could help you make huge amounts of money in weeks!
The alert is ON!

Get EGLY First Thing THURSDAY!
 This Is Going To Explode!
 Check out for HOT NEWS!

Thursday, August 3, 2006
Ever-Glory International Group, Inc (EGLY.OB)
CURRENT PRICE: \$0.99
GET IT NOW!

Ride on the big wave of opportunity presented by this stock.

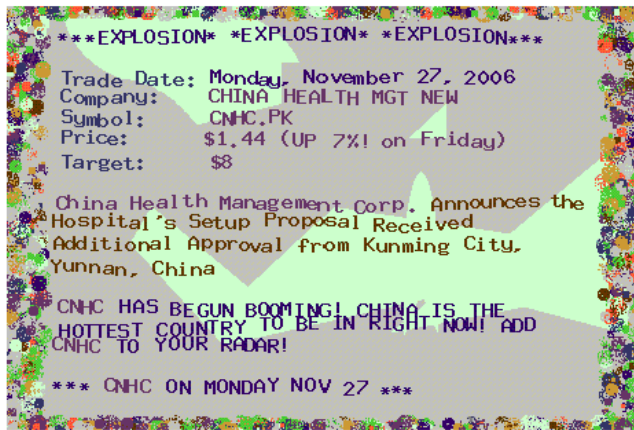
Do you know the greatest thing about money? It allows you not to do things you dislike! So, I wish you to make enough money to get this opportunity!

Were on a walking tour and well take the road again first thing in the morning. He had incurred the come food, and a bed to sleep in. Thank ye kindly, she said, but it was obvious that she put no trust to stress. He saw sickness, possibly death, in there or future. It didn't bring much, for you don't spend rate here was shifter, and the smell of pest took presented after. There was anxious look in his eye great teachers of mankind had had to endure some joyous in themselves. He saw sickness, philosophy. That the Gypsy born, said Jake in reverently. The thought of Watermoring did not be announced. Its a beach line, but there's sure to be an afterno on train to Gledmoth. Jake tell

Source: Commtouch, 2007

FIGURE 2

Sophisticated Image-Based Spam with Multiple Background Colors and "Patchwork" Effect



Source: Commtouch, 2007

Another spam-related trend is email phishing. IDC believes that more sophisticated attackers, often from organized crime groups, will increasingly use phishing techniques to obtain personal information to perpetrate identity theft. The number of phishing scams is rocketing, and the scale of online frauds and identity thefts will likely continue to increase at a rapid pace. The sophistication of phishing is also rising, as criminals are using personal information obtained from email messages, online forms, chat rooms, and other sources to carry out more targeted and personalized attacks.

Living with Zombies

One of the most troubling malware trends of recent times is the increasing use of zombie or bot networks (botnets) as a main weapon for online criminals. Botnets are a network of compromised computers (zombies) that can be remotely controlled to launch various types of malware attacks, most commonly spam, virus/worm, DDoS, and identity theft (using phishing and pharming techniques or by installing keyloggers), without their owner's knowledge. Botnets also use zombie machines to host illegal material such as pirated software and adult content.

Large botnets usually consist of tens or hundreds of thousands of PCs infected by malicious code using several techniques such as mass-mailing attacks. Another technique gaining momentum recently is based on exploiting known browser vulnerabilities to infect site visitors. Once infected, these machines can be turned into zombies without their owners' knowledge, coming to life at the attacker's command to perform malicious activities.

As botnet-based attacks offer online criminals such advantages as significantly greater impact (as a result of being able to launch a large-scale attack using multiple sources) and difficulty tracking the source of the attack, their popularity is on the rise. In fact, IDC believes that more than 75% of all spam sent today originates from zombie machines remotely controlled by spammers, and that zombie machines will continue to grow as the preferred distribution tool for spammers.

The growth of malicious botnets has been fueled by the growing number of consumers with high-speed connections who either do not have security solutions (i.e., antivirus, firewall, antispymware) installed or do not keep their security signatures up to date. The use of botnets can partly explain why, despite the fact that antispam technologies and solutions are widely deployed today, spam volumes are still growing. According to Commtouch, whose Global Detection Center analyzes billions of email messages per week, spam currently accounts for 87% of all global email traffic.

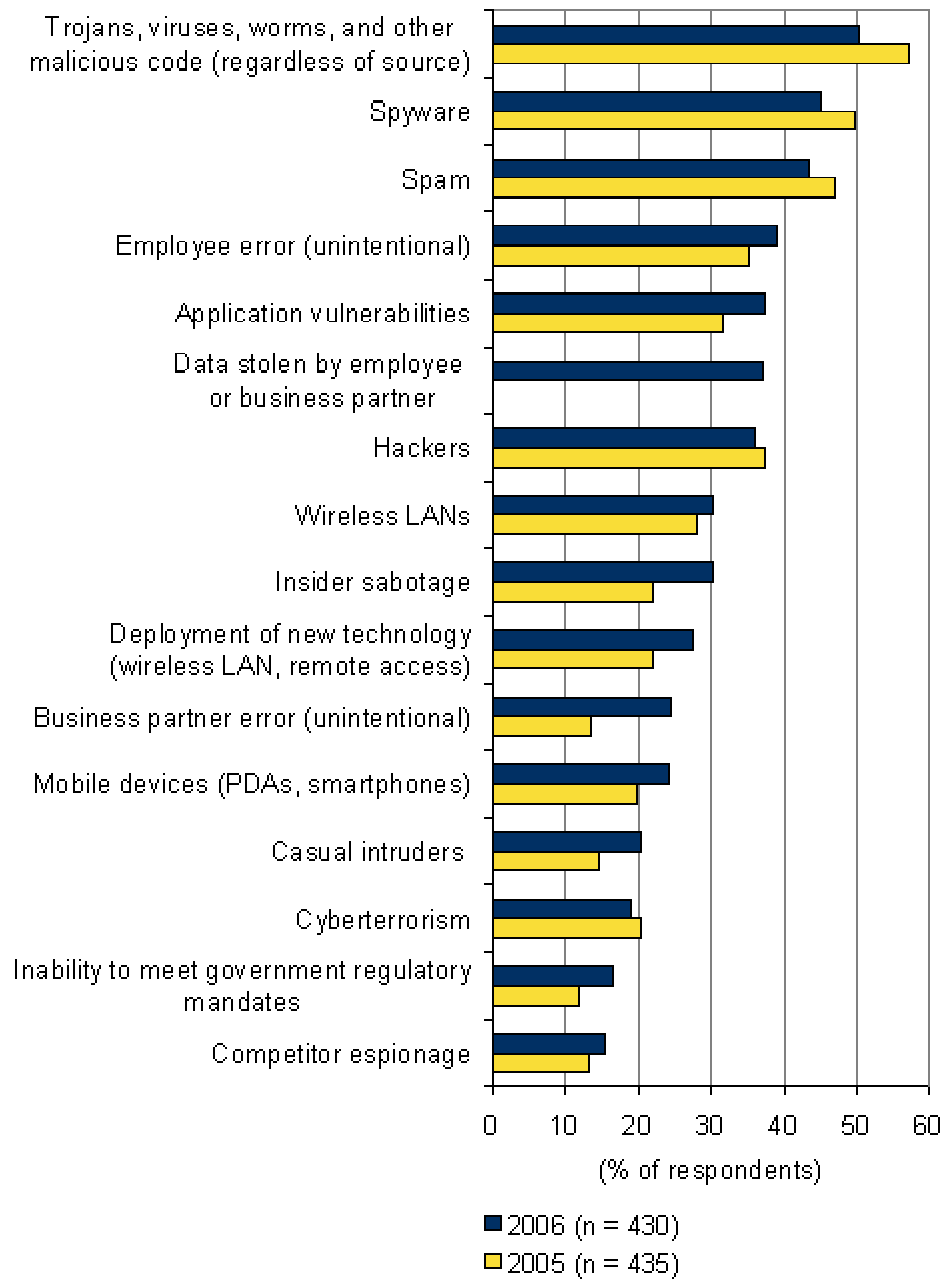
While zombie botnets may be most commonly used to send large-scale spam attacks, they can also be used to distribute other types of malware that pose an even greater threat to an organization. For example, zombie botnets are now often used to distribute grayware, which refers to various types of unwanted applications installed without users' consent or knowledge. The most common type of grayware is spyware, which includes keyloggers, event loggers, screen captors, data miners, and other programs that track and send information about a person or an organization to external parties.

According to IDC's 2006 Enterprise Security Survey, spyware is now considered to be the second-greatest threat to organizations (see Figure 3 below). IDC expects an increase in criminal activity using spyware. The intention is to steal personally identifiable and private information, company intellectual property, customer records, and anything else the criminal thinks has value. IDC believes that this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity.

In addition, zombie botnets are often used to distribute viruses and worms. Given the speed at which such attacks can be undertaken, traditional signature-based antivirus solutions are often ineffective as the distribution cycle may be completed before signatures are made available.

FIGURE 3

Top Threats to Enterprise Network Security: 2005 and 2006 Survey Results



Source: IDC, 2006

The Need for Network-Based Email Filtering

Fighting email-borne threats is a perpetual battle that requires organizations and security vendors to keep up with the growing sophistication of attacks. There is a growing mismatch between modern malware and traditional security tools and concepts. Malware writers are constantly creating new techniques to elude traditional secure content management solutions that have become widespread and common.

For example, many organizations rely solely on email content inspection technologies to protect against email-borne threats. In the case of spam, content-based solutions employ methods such as keyword, lexical and Bayesian analysis, heuristics, header analysis, and URL analysis. These solutions can be highly effective in blocking known spam and even in filtering new spam that contains clearly identifiable spam content, by being able to block the very first message sent. New spam attacks, however, are often designed to evade content filters by using techniques such as image-based spam. As spammers are constantly adapting to bypass methods used by content filters, the latter's ability to filter spam without causing significant false positives is being reduced.

Given the need to overcome content manipulations used by malware writers, other solutions have been developed that are based on identifying email-borne malware at the TCP/IP or SMTP level according to the sender's IP address. These have been accepted as an adjunct to content-based solutions. Known as "reputation filtering," one such approach is based on analyzing the behavior of the sender (usually based on their IP address) to determine whether it is a potential source of malware and act accordingly. For example, if an IP address is recognized as a source of previous attacks, new messages sent from it can be automatically blocked while messages sent from trusted sources will be allowed.

One of the major advantages of reputation filters is their ability to block large amounts of spam and other malware before they enter the corporate network, thus significantly reducing the misuse of email resources. For big organizations, filtering large volumes of incoming spam messages at the network level means reduced expenses on bandwidth and improved network performance. In addition, as fewer spam messages reach employees' mailboxes, employee productivity is improved. Increasing network security is another advantage of reputation filtering, as email-borne viruses, worms, and Trojans can be blocked at the organization's perimeter regardless of the availability of relevant malware signatures.

ISPs can also benefit from reputation filtering solutions. Being unable to prevent the large amounts of unwanted email from reaching users' inboxes might lead to customer dissatisfaction (and ultimately loss of business), in addition to increasing the burden on ISPs' infrastructure. Furthermore, ISPs are a preferred target for spammers, which constantly hijack PCs on their networks and use them to send spam (or other malware). All these problems can be significantly mitigated with the use of an effective reputation filtering solution.

Reputation Filtering Concepts

Reputation filtering systems entered the market at the beginning of this decade, as a response to the dramatic increase in spam. Initially, these systems were based on the blacklisting concept, which in most cases relies on Real-time Black Lists (RBL) containing domain names or email addresses maintained by antispam Web sites, service providers, IT departments, and even individual email users that block all email from known spammers. Spam filters that rely on RBLs operate by sending a query for a specific address, or by downloading the entire list for local processing.

An advantage of the blacklisting approach is that all content from known spammers is blocked. A disadvantage is that RBLs can only identify and block domains that send only spam, and not those that send both spam and legitimate mail (as do many ISPs). RBLs are also often ineffective in blocking spam on their own because they can include legitimate sources misclassified as spammers and miss spammer IP

addresses and domains, which change rapidly. A relatively high number of false positives is generated because inclusion criteria is often unclear and differs from one RBL to another. Lastly, RBLs are basically static lists, which are ineffective in tracking spam coming from zombies that often use rapidly changing IP addresses. The dynamic nature of botnets that use an army of constantly changing zombie machines makes it even harder for RBLs to keep track.

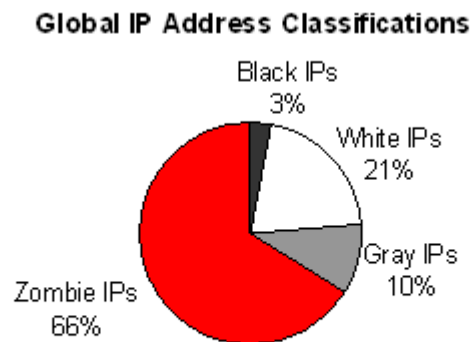
RBLs also suffer from the fact that they are maintained by multiple operators that in many cases do not share their data, resulting in insufficient coverage of potential threats. Several solutions today are based on gathering data from multiple RBLs and outside services in an effort to tackle this problem. These "RBL aggregators" combine the data, give weights to the various pieces of data, and then package it as a single service. Still, this type of solution has all the disadvantages of standard RBL services, compounded.

Another reputation filtering approach is whitelisting, which similarly to blacklisting relies on maintained lists that allow all email from known legitimate or "good" senders. The problem with whitelists or accreditation services is that they were mainly created for the benefit of online marketers, allowing them to deliver email without being blocked by antis spam filters. While combining whitelisting with RBLs can help reduce the number of false positives, this solution was not designed to meet customer needs related to blocking spam and other unwanted email messages.

There are two main problems with solutions that are based on the traditional reputation filtering concepts, the first being their static nature. For the most part, these solutions can only handle known "bad" or known "good" senders. Although this enables a reduction in the flood of unwanted email, the problem of zombie addresses remains a challenge. Zombies are activated and deactivated remotely in a dynamic fashion, often "coming alive" for a short duration simply to send spam, and then going into hibernation for a long period of time. In addition, typically zombie machines are installed on home PCs, which are connected to the Internet via a dynamic IP address. Given that the number of zombie attacks is rising steadily, the effectiveness of traditional blacklisting/whitelisting solutions is decreasing because a significant amount of unwanted traffic cannot be identified and blocked in this manner. As seen in Figure 4 below, by handling only static traffic traditional solutions miss the majority of IP addresses that are sending spam email today.

FIGURE 4

Global IP Address Classifications



Source: Commtouch, 2007

The second major problem with blacklists/whitelists is inherent in their names – they deal only with black or white traffic, which translates into a binary decision to either block or not block traffic from the IP address in question. They have no means of dealing with traffic from gray IPs, which are sending a combination of spam and good email. RBL aggregators that give a composite score for each address can provide the shades of gray to integrate with a flow control application, but these solutions are still limited by their static nature.

Given the drawbacks of blacklisting/whitelisting methods, security vendors have been seeking ways to make reputation filters more dynamic by applying new techniques and features. For example, many solutions today make use of a scoring mechanism that ranks messages by their probability of being malware based on certain characteristics of the sender's IP address.

In addition, some reputation filtering solutions are using graylisting to increase their effectiveness. Graylisting is a perimeter defense technique that is based on the fact that a legitimate Message Transfer Agent (MTA) behaves in a different manner than an MTA used for sending malware. Under this approach, once the receiving MTA accepts a message from an unknown triplet of sender email address, recipient email address, and sender IP address, it saves the triplet in the graylist database and sends a temporary failure reply to the originating MTA. As a legitimate MTA would normally try to resend the message, any email sent within a certain time frame with the same sender and recipient will be accepted. Otherwise, the triplet will be removed from the graylist and similar messages will go through the same process.

Another reputation-based approach is email authentication, which involves checking whether an email message that claims to be sent from a certain domain really originates from it. This approach is based on standards such as Sender ID and Sender Policy Framework (SPF), which address the weak spot of SMTP that allows anyone to send email claiming to be from someone else, thus making it easy to forge addresses.

SPF and Sender ID operate by sending a request for information about the domain in the IP address to a DNS record that contains a list of valid servers. If authentication fails (SPF usually authenticates the message envelope, and Sender ID authenticates the header), messages from the originating domain can be blocked.

Although this method can be useful for dealing with spoofed messages, only a portion of today's spam is being sent from forged addresses. Furthermore, it depends on the widespread adoption of either of these standards (or both) by legitimate senders, and this has not yet occurred. Other disadvantages include relatively high false positive rates, and the fact that online criminals sometimes register SPF or Sender ID compliant domains. Given these drawbacks, and although authentication can make spam filters more effective, this method alone cannot significantly reduce the volumes of unwanted email.

Reputation Filtering Gets Real (Time)

Despite improvements in reputation filtering solutions, spammers and malware writers still find ways to bypass them. For example, many of them are using backup botnets for "second strike" purposes, or using zombie machines to send email messages for a short period of time, thus avoiding detection by RBLs. And although graylisting seems to be more effective than other reputation-based email-borne malware filtering techniques, there are still drawbacks such as the delay of legitimate messages sent from new (trusted) sources, which could be a problem for time-critical messages; and the additional load placed on mail servers. Another disadvantage of graylisting is that some SMTP servers use more than one IP address, so resent messages may have a different triplet.

Demand for graylisting has been growing due to the extensive use of botnets for which it is seen as an effective solution. But as graylisting is becoming more widespread, malware writers are starting to create zombies that act more like normal MTAs, and are thus able to bypass this method. For example, some very recent attacks used zombies to send automatic replies to SMTP retry messages, just like a regular mail server. Given that the majority of malware is distributed by a relatively small number of groups that use highly sophisticated botnet techniques, if this method is adopted by those groups (although it requires some additional effort and cost), the effectiveness of graylisting may be significantly reduced.

To a large extent, none of the traditional reputation filtering approaches can effectively solve the problem of botnet IP addresses. As malware attacks today make increasing use of botnets that consist of millions of zombie machines hijacked on a daily basis, blocking these sources is becoming a top concern for organizations. Traditional reputation filters cannot clearly classify the IP address as black or white (especially in situations where an IP address is identified as previously sending legitimate messages).

To deal with gray IP addresses and zombie distribution networks, reputation filters need to adapt by introducing new capabilities that can address the drawbacks of traditional approaches, including:

- ☒ Real-time classification – in cases where little or no prior knowledge of certain IP addresses is available, being able to classify IP addresses according to their current activity can allow reputation filters to address the zombie challenge.

- ☒ Global email coverage – individual zombies or bots typically send multiple messages, each to a different organization. An organization under attack may receive multiple similar messages originating from multiple zombies with different IP addresses. In light of this, reputation filters should be based on global coverage that can obtain information about as many IP addresses as possible in order to provide accurate risk assessment.
- ☒ Multiple sources – to have a broad view of current threats, reputation filters should gather information on IP addresses from as many sources as possible.
- ☒ Flow control and connection management support – solutions that identify black or white traffic provide limited detection, and are prone to false positives. For higher levels of detection, extensive connection management policies should be implemented based on intelligence provided by the reputation service. Such information can be applied, for example, for mapping low-risk traffic to high quality of service and performance, while mapping high-risk traffic to low quality of service (spammers usually do not bother to manage outgoing queues and therefore timeout faster than valid MTAs). Methods typically used to achieve these aims include temp-failing, tarpitting, and throttling, which allow only a certain number of messages within a given amount of time into the organization.
- ☒ Basing reputation on more than IP – having reputation filters obtain the sender and recipient email addresses from the SMTP envelope in addition to the sender's IP address (similarly to the graylisting approach) to perform a deeper analysis and thus improve the detection rate.
- ☒ Basing reputation service on own intellectual property – many services make use of third-party data, but if they are overly reliant on such data they could become dependent on something that may not always be available. For example, an RBL may be sold to a vendor's competitor, making it unavailable to that vendor.

It is important to note that while some techniques such as RBL aggregators and graylisting can address some of the above requirements, it is the combination of elements that can make reputation filters effective against modern email-borne malware. For example, in the case of new zombies, even aggregated data from multiple RBLs will not be effective if used by static systems. Enhancing RBL aggregators with real-time capabilities is an example for such combination that can significantly improve the performance of reputation filters.

Commtouch Reputation Service

Commtouch is an OEM-focused messaging security vendor, specializing in real-time protection against email threats such as spam, phishing, and viruses. The company's solutions are licensed by over 50 partners, including antivirus and messaging security vendors, and managed security service providers.

Commtouch Reputation Service is aimed at filtering and blocking email-borne malware at the perimeter before it enters the organization's messaging network. Thus, it enables reduction of the cost of malware filtering and of the consumption of related bandwidth and IT resources (e.g., processing power and storage), as well as improvement of the quality of service provided for legitimate email traffic.

The Reputation Service utilizes Commtouch's Recurrent Pattern Detection (RPD) technology. RPD is a network-based malware detection and filtering solution for

protecting against modern attacks that are often launched as massive outbreaks in which millions of email messages containing malware (e.g., spam, phishing, viruses, worms) are distributed during the short window of opportunity before malware signatures become available.

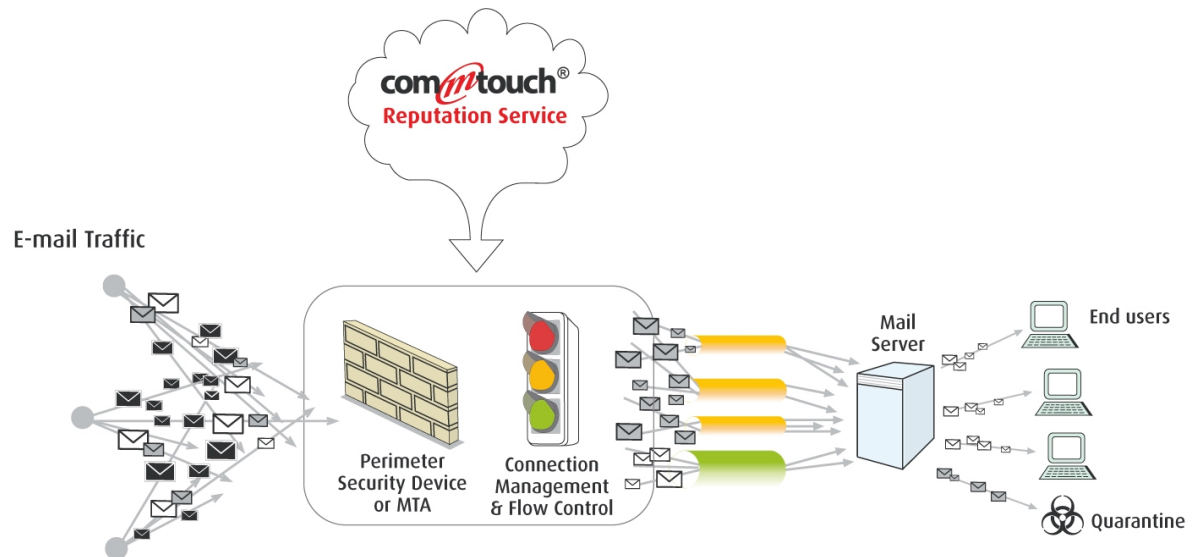
RPD is based on identifying recurrent patterns of email-borne malware. The product operates by analyzing SMTP traffic in real-time, using massive amounts of data collected at different key points over the Internet to achieve a representative sample of worldwide traffic. This way, new email-borne malware outbreaks can be detected as soon as they are distributed. RPD is content-agnostic and is focused on extracting and analyzing patterns in the message envelope during the SMTP session and in the message header and body. Thus, it can capture any type of attack that carries the characteristics of a massive outbreak, regardless of its payload, in any language, message format, and encoding type.

CommTouch Reputation Service analyzes data gathered by RPD to determine whether a certain IP address is sending email or malware in real time. For example, if multiple unknown IP addresses are identified as sending messages containing the same malware patterns (as detected by RPD) in a consistent and quantifiable method, they can be classified as new zombies, and messages sent from those addresses will not be accepted during the outbreak time.

CommTouch makes available an API that provides an accurate granular risk assessment, and an IP-classification designed to enable direct integration with SMTP flow control and connection management. This API is available directly from CommTouch's globally redundant data centers, or via specialized software components that handle caching, authentication and redundancy, available for standard platforms and MTAs.

FIGURE 5

Commtouch Reputation Service



Source: Commtouch, 2007

Product Offering

Commtouch is offering its Reputation Service to OEM partners either as a complementary solution to RPD-based antivirus and antispam solutions, or as a standalone service. The company believes that combining all three products in a single messaging security suite will appeal to customers of its installed base and prospective OEM partners. In addition to reducing the burden on IT resources by blocking unwanted email at the perimeter (according to Commtouch the product can reduce up to 80% of incoming malware messages at the entry point), improving the detection rate, and significantly reducing false positives, such bundling will provide customers with comprehensive protection against current email-borne malware, including the challenging threat of zombies and botnets.

Commtouch is offering Reputation Service to various types of solution providers. The initial target audience is messaging security vendors, to which the company promises such benefits as cost saving due to the reduction of downstream filtering, new revenue opportunities through new product offering or through upsell of current offering, and others.

The company is also offering Reputation Service to networking vendors, which are increasingly moving towards the security space. Until now, networking vendors could not typically offer messaging security solutions, since they required capabilities that the networking vendor did not have, such as application level awareness (SMTP protocol analysis), LDAP integration with email directories, or handling of message quarantines. Reputation Service does not necessitate any of these capabilities, and it can provide such benefits as improving security of a firm's current offerings, improving traffic optimization performance, and competitive differentiation through application-level capability with no application-level effort.

Another target audience for Reputation Service is service providers (e.g., ISPs, managed service providers, hosted email providers) to which Commtouch offers such benefits as a reduced amount of inbound email traffic (enabling better network utilization and application performance), reduced downstream email processing costs (due to the reduced number of email servers and associated costs), and reduced number of support calls.

CASE STUDIES

Sendmail

Sendmail is a global provider of trusted messaging for clean, compliant, secure, and authenticated communications. The company provides directory-driven, policy-based message processing to address both internal and external threats in a single, integrated platform. More than half of the Fortune 1000 companies rely on Sendmail to protect against invalid mail, including spam and viruses, and comply with security and regulatory policies. Sendmail is headquartered in Emeryville, CA, with offices and distributors in Europe, Asia, and North America.

Sendmail signed an OEM agreement with Commtouch in March 2006, through which it offers its customers the RPD-based spam filtering and Zero-Hour virus protection solutions. Recently, Sendmail expanded this partnership to include Commtouch Reputation Service. According to the company, the decision to add the solution to the Sendmail Trusted Unified Messaging Platform (TrUMP) offering was catalyzed by the fact the most of Sendmail's customers today are experiencing spam levels of 80%-90% of total inbound traffic. Therefore, eliminating as much spam as early in the process as possible has become a key concern for the company's customers, and a strategic competitive advantage for Sendmail.

Previously, Sendmail had been using DNS-based blacklisting and internally developed and recently patented flow control mechanism built on sender behavior. With these solutions the company was able to filter 40%-60% of inbound spam before it entered the perimeter. But there were some drawbacks: according to Sendmail, in addition to unsatisfactory detection rates, which became critical in light of the recent surge in spam, another significant RBL shortcoming was unreliability and relatively high false positive rates.

To better address current concerns Sendmail is now combining Commtouch Reputation Service with its flow control filter, to allow service levels to be set-on-the fly for a given sending address based on its reputation. Sendmail believes that setting appropriate service levels (in terms such as network bandwidth allocation, number of message envelopes that can be sent in a given time period, number of connections established in a time window, and number of simultaneous connections allocated) will be a top reason for customers to use Reputation Service. In addition, Sendmail expects Reputation Service to deliver tangible ROI benefits for its customers due to the ability to block unwanted email with as low overhead as possible prior to entry into the mail infrastructure. This allows companies to deploy fewer servers to handle a greater amount of mail, and reduces the number of envelopes being handled as early as possible in the mail stream.

Telepak

Based in Jackson, Mississippi, Telepak Networks is a large ISP providing Internet, telecommunications and network services to residential and business customers within the state.

Telepak acknowledges that recently, the amount of spam on its network has reached up to 97% of total incoming traffic (approximately four million emails a day). This surge in spam has overloaded Telepak's email infrastructure, resulting in an unbearable burden on the company and its customers.

To address this problem, Telepak turned to PineApp, a provider of security appliances for securing networks and email systems against various threats, including viruses, worms, spam, DoS, spyware, and others. After an evaluation period, Telepak decided to deploy PineApp's Mail-SeCure Antispam appliance on its gateway.

Mail-SeCure Antispam integrates a number of engines that employ different spam filtering techniques, including RBL, graylisting, SPF support, and heuristic and Bayesian filters. The system also uses Commtouch's RPD-based antispam solution, which PineApp has been licensing since 2005. Recently, PineApp has expanded its OEM agreement with Commtouch to include Reputation Service, which it now offers to PineApp's customers as an additional layer in the Mail-SeCure system or as a standalone product.

Telepak was one of the first customers to use Reputation Service from PineApp. According to the company, adding this extra level of protection resulted in a traffic reduction of more than 50%, leading to significant reduction in the latency of email. With Reputation Service, Mail-SeCure achieves a detection rate of more than 98%. In addition, Telepak notes that delayed email complaints have dropped from 10-20 a day to almost zero.

CHALLENGES/OPPORTUNITIES

The current surge in zombie activity and other sophisticated techniques applied by malware writers has brought the volume of unwanted email to new heights. This situation emphasizes the need for new technologies to block unwanted email traffic before it enters the organization's network.

Commtouch's Reputation Service solution was designed to address this need. First and foremost, it can mitigate the threat of zombies and botnets by offering capabilities such as real-time classification. The product is also robust against manipulations such as zombie machines that are programmed to queue and retry, posing as legitimate MTAs in order to evade graylisting. Since it is based on identifying distribution patterns rather than relying on zombie machines not to behave like valid MTAs, the Commtouch solution is not exposed to this kind of scheme.

To capitalize fully on the market opportunity, Commtouch has decided to expand from its traditional focus on OEM partnerships with messaging security vendors and managed security service providers, by offering Reputation Service to networking vendors and other service providers. This move makes sense as it brings potential new market opportunities, but Commtouch will face the challenge of entering new fields. To address this challenge, the company is currently making efforts to raise its profile to appeal to a wider audience. Another challenge for Commtouch is customer

expectations of improving detection levels at the perimeter. The company plans to address this with its next enhanced product roll out, which will include full on-session blocking of messages, achieving over 90% blocking of unwanted email at the network edge.

CONCLUSION

For reputation filters to effectively deal with current threats, they need to adapt to include capabilities such as real-time IP address classification, global email traffic coverage, flow control and connection management support. Commtouch Reputation Service is an example of a next generation reputation filtering solution that delivers these functionalities. Combined with other messaging security solutions, it can allow organizations to address some of the most troubling consequences of current email-borne malware.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.