Ipswitch IMail Server with Integrated commtouch® Technology

As spammers grow in their cleverness, their means of inundating your life with spam continues to grow – very ingeniously. The majority of spam messages these days attempt to breach security and offer a host of threats on a computer reading the message or redirect the user to a website full of malware. Although many methods to combat these threats have been developed and tested throughout the past several years, a common deficiency of most of these methods is that they lack the ability to adapt quickly enough to the rapid change of distribution and infiltration techniques invented by spammers and virus authors.

Real Security. In Real Time.

Problem

Many spammers attach viruses to email in an attempt to gain access to all the vital information stored on computers. Over recent years, spam and malware attacks have cost global businesses billions in damages, an amount that continues to rise each year.

Lost messages and data due to improperly configured filters and blockers that weed out legitimate business correspondence, also put a price tag on businesses cost. Presently, it is becoming clear that malware authors, spammers and phishers are learning from each other, and forming various kinds of partnerships such as trading or selling personal email information and mailing lists.

Spam Detection

Spammers typically produce spam for commercial gain rather than malicious intent. Although the purpose may be to sell a product or service to recipients, spammers often use unethical methods to acquire email addresses of recipients and to distribute mass mailings. In composing spam messages, spammers use sophisticated tactics to evade existing spam detection applications. This includes covering the tracks leading back to the spammers, manipulating or hiding the commercial URLs, using non-English words and phrases and a host of other methods.

Typically a massive spam outbreak will only last a few hours and can be launched from a network of 'zombie' machines. To complicate the detection process, each message within the massive spam outbreak can be composed differently and employ more than one evasion technique.

Phishing Detection

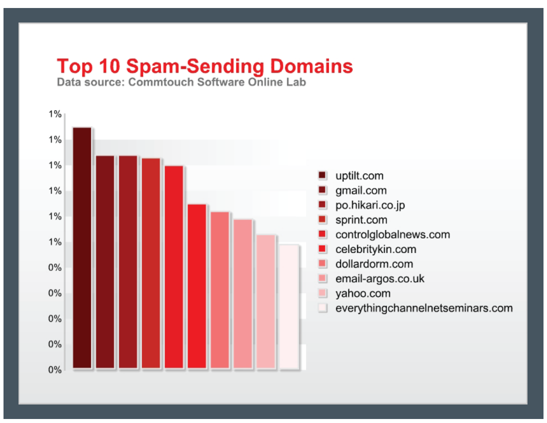
Password harvesting, or phishing messages, are typically sent for the single purpose of identity theft. There is an underlying intent within each message to violate the privacy of the recipient and commit fraud. The goal of a phishing message is to fool the user to go to a web site which will request them to enter private information. By using highly effective social engineering methods, these messages target users, often with a sense of urgency, to believe they have arrived at a legitimate site such as their bank or recognized online vendor to enter their private information. The sender is then able to gather personal information such as credit card numbers, passwords, social security or identification numbers and other private information.

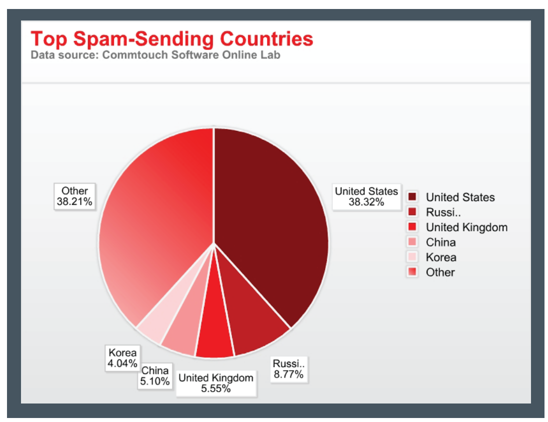
Phishing messages appear to be from genuine or credible sources. Like spam, phishing messages can be sent in any language or format in attacks that typically last only a few hours and are usually launched from an army of 'zombie' machines on the Internet.

Image-based Spam*

Image-based spam places a significant burden on an 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. Image-based spam peaked in 2006 and 2007 and accounted for 35% of all spam on average (compared to less than 10% in 2005), which brought 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.

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.





** Image-based spam is not as prevalent as it once was. However, there is no current ability to predict the course of future spam trends. Therefore, we are including this section to demonstrate Commtouch's ability to properly handle image-based spam.*

Message Patterns

Massive outbreaks which distribute spam, phishing, and email-borne viruses or worms, consist of many millions of messages intentionally composed differently in order to evade commonly-used filters. Nonetheless, all messages within the same outbreak share at least one and often more than one unique, identifiable value which can be used to distinguish the outbreak.

For example, in the case of spam the objective is to lead the recipient to the same commercial web sites that can be classified as spam. In doing so, different spam attacks are often launched from the same network of zombie machines that can be blacklisted. In the case of phishing, recipients are lured to voluntarily disclose personal and confidential information via clever social engineering methods and the objective is often to lead the victims to same faked URLs. These values are called the 'message patterns' of the outbreak. Any message containing one or more of these unique patterns can be assumed with a great deal of certainty to be part of the same outbreak.

Message patterns are extracted from the message envelope, headers, and body with no reference to the lexical meaning of the content. Thus pattern analysis can be used to identify outbreaks in any language, message format, and encoding type. Message patterns can be divided into distribution patterns, which determine if the message is 'good' or 'bad' by analyzing the way it is distributed to the recipients, and structure patterns, which determine the volume of the distribution.

The challenges of message pattern classification are in determining which message patterns identify outbreaks without generating cases of false positives, and how to extract and analyze these patterns before the outbreak wanes. Most outbreaks have a relatively short lifecycle measured in only a few hours. Therefore, any solution that does not detect and classify messages in real-time will only be effective towards the end of the outbreak, when most of the damage has already been done. All outbreaks attempt to disguise messages as legitimate email correspondence pretending to arrive from trusted sources and therefore, solutions that are based on pattern analysis must be able to tell the difference between 'good' and 'bad' patterns and avoid making mistakes.

The challenges are made more complex by the fact that each new outbreak usually introduces completely new patterns that were not previously analyzed and are therefore unknown to the pattern analyzer. Pattern detection represents a new and greater understanding of how email-borne threats are created and propagated. Because tactics for distributing spam and phishing are constantly evolving, it is necessary to proactively identify new and unique patterns in real-time in order to determine new outbreaks as they are released to the Internet and begin targeting recipients.

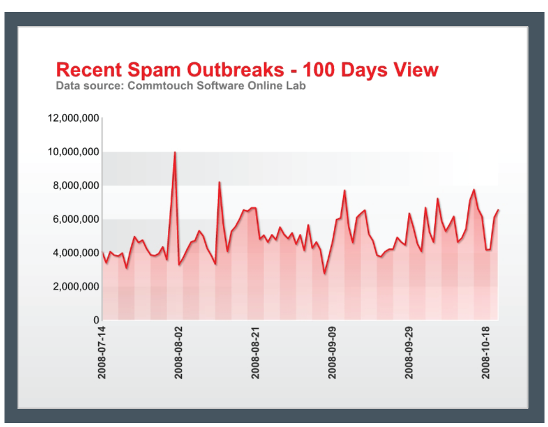
Understanding IMail Server with CommTouch

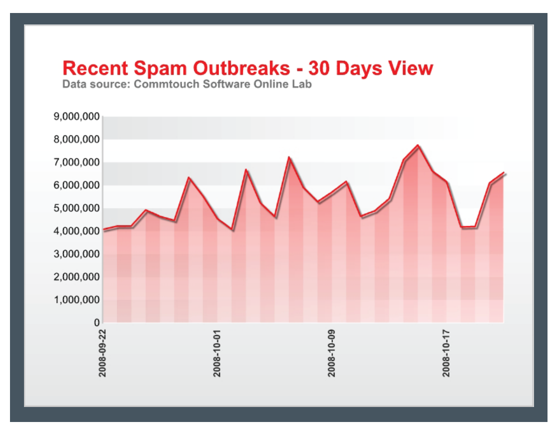
IMail Server Premium utilizes Commtouch technology to provide industry-leading protection for your business.

Commtouch's Recurrent Pattern Detection (RPD) technology, based on the identification and classification of message patterns, delivers the highest threat detection capabilities.

The Commtouch approach is based on the understanding that all threat outbreaks share some common characteristics, including:

- Most email messages within the outbreak have been altered to make it difficult to set blocking rules based on lexical analysis.
- Most outbreaks include millions of email messages to maximize the highest possible response rate and the greatest ROI for the attacker.
- Most outbreaks are released within a short period of time, requiring a real-time solution to detect the outbreak to limit or avoid the damage that can be incurred.
- The originators of the attacks invest heavily in disguising their origin to make it difficult to track the message back to them.





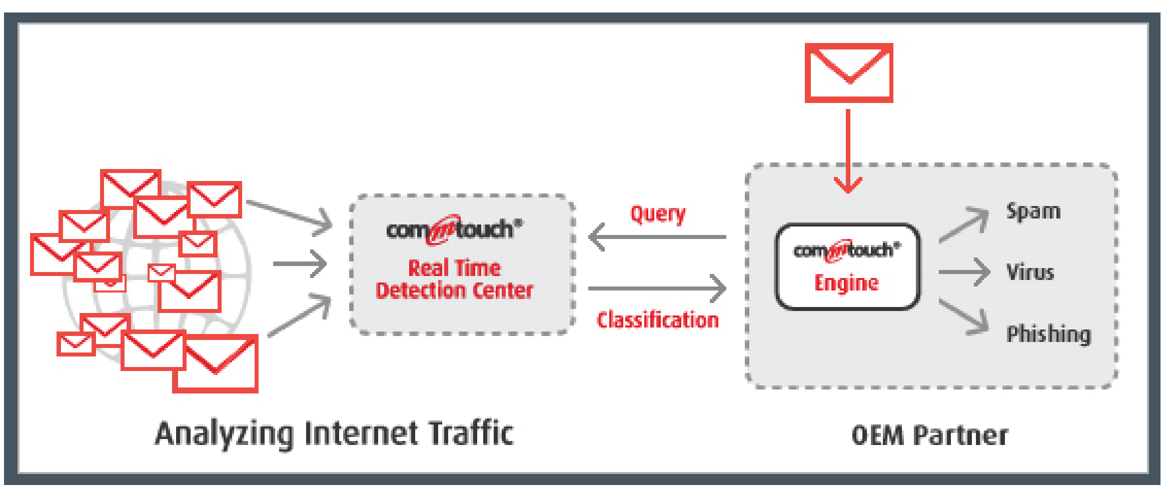
How the Product Solves the Problem

Recurrent Pattern Detection (RPD) technology detects and classifies all types of email-borne threat patterns in real-time. RPD is hosted by the Commtouch Detection Center, which proactively analyzes vast amounts of Internet traffic in real-time.

RPD, based on Commtouch's U.S. patent #6,330,590, extracts and then analyzes relevant message patterns, which are used to identify massive email-borne outbreaks. RPD classifies both distribution patterns and structure patterns and the analysis results are stored in a vast warehouse of classifications. In addition to identifying new threat patterns, RPD is also used to modify or enhance classifications of already-identified message patterns.

RPD is designed to distinguish between the distribution patterns of solicited bulk emails which represent legitimate business correspondence, from those of unsolicited bulk emails by applying a reverse analysis. The results of this analysis are 'bleached' message patterns belonging to 'good' messages such as popular newsletters, mailing lists, etc.

Commtouch uses the RPD technology in a highly scalable environment to deliver extremely high performance rates by analyzing many millions of new patterns each day, (24x7x365). New outbreaks are identified within minutes since they are launched on the Internet globally.



Reputation Filtering

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.

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.

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.

Conclusion

To effectively combat email-borne threats, a successful solution must address a growing number of challenges.

Commtouch's RPD is a proactive detection technology that continues to outwit those who continue to invent new methods to propagate email-borne threats because it does not rely on the contents of the email and therefore, it is able to detect spam in any language and in every message format (including images, HTML, etc.), non-English characters, single and double byte, etc.

RPD technology offers:

- High spam detection rate with almost no cases of false positives
- Protection against phishing attempts
- Content-agnostic threat protection
- Multi-language threat detection
- Multi-format threat detection

For these reasons, the RPD technology is the best companion to messaging and security applications to provide real-time protection against spam and malware.

Along with RPD technology, reputation filters have the 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.

For reputation filters to effectively deal with current threats, they need to include capabilities such as real-time IP address classification, global email traffic coverage, flow control and connection management support. Commtouch GlobalView™ Mail 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.

About Ipswitch, Inc.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading Ipswitch WS_FTP® Professional client and Ipswitch WS_FTP Server and communicate via Ipswitch IMail Server.

To view the IMail Server blog, visit
http://blogs.imailserver.com/.

For product and sales
information, visit http://www.imailserver.com.

About Commtouch

Commtouch Software Ltd. (NASDAQ: CTCH) is the source of proven messaging and web security technology for scores of security companies and service providers, founded on a unique datacenter-based approach. Commtouch's expertise in building efficient, massive-scale security services has resulted in its patented technology being used to mitigate Internet threats for thousands of organizations and hundreds and millions of users in over 100 countries. Commtouch's Data Centers automatically analyze billions of transactions in real-time to identify new spam, malware and zombie outbreaks as they are initiated. Commtouch's unmatched suite of security offerings - anti-spam, virus detection, reputation and zombie intelligence services - work together in a comprehensive feedback loop. Commtouch was founded in 1991, is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif. For more information and real-time statistics and trends, see: http://www.commtouch.com and the Commtouch Café blog at: http://blog.commtouch.com/cafe.