Anti Spam – Best Practices

Anti Spam LIVE Service:
Zero-Hour Protection

An IceWarp White Paper

October 2008

www.icewarp.com

Background

As discussed in the IceWarp white paper entitled, "Anti Spam Engine: Trusted Real-Time Scanning," spam is a dilemma of modern communications that will not go away. Unchecked, the cost to business would be staggering.

> By June 2008, 96.5% of all email in the average business server was spam.
>
> -- *Sophos*

The cost has many faces:

- Increased operational costs
- Loss of productivity
- Breaches in security
- Cost in downtime
- Loss to reputation & customer confidence
- Legal liability

The best defense is an aggressive, technologically sophisticated, counter-campaign – not one that relies *merely* on traditional updates of spam definitions, but one that also provides zero-hour real-time accuracy. Since spammers are getting savvier, the strongest antispam solution is one that adapts as outbreaks occur.

Commtouch's Q2 2008 threat report indicates that, on average, 77% of all email is bona fide spam. During this time, the rate went as high as 94%. Spam will not go away; on the contrary, the number of spammers is always increasing, and spammers as a whole are becoming more aggressive, resilient and determined.

Through the employment of zombie networks (botnets), spamming is becoming a fulltime, fully automated activity, seizing systems and hurting businesses and end users. Commtouch's findings indicate that there are 10 million zombie IP addresses in use each day. Zombie networks cannot be ignored as they are the dominant method of spam delivery.

Spam is not just a nuisance; it is often *malicious*, secretly hijacking corporate servers and turning *them* into spamming systems that spammers control remotely. A server that has been compromised quickly results in the blacklisting of the sending IP address. As a consequence, both inbound and outbound communication comes to a crawl. Even legitimate email sent from the server will be rejected by receiving systems.

Getting a system removed from a black list can be very time consuming and costly.

IceWarp Anti Spam LIVE offers the most sophisticated and comprehensive protection. Not only does it check inbound email – it also verifies that outbound email is legitimate. Spam that is found on the system is either deleted or rejected, depending on administrative settings.

What is Anti Spam LIVE?

Anti Spam LIVE is one of the latest technologies integrated into IceWarp Server. This service provides IceWarp users with real-time spam scanning and tracking, courtesy of Commtouch technology.

IceWarp engineers integrated this innovative technology into IceWarp's standard antispam engine, resulting in spam identification that reaches or exceeds 98% accuracy. More spam is filtered out while the rate of false positives decreases.

Commtouch® Software Ltd. (NASDAQ: CTCH) was founded in 1991, and is dedicated to protecting the integrity of the world's most widespread form of communication, email. With over sixteen years of expertise in the development of email software, Commtouch provides spam and Zero-Hour virus outbreak protection for tens of millions users in 130 countries. Commtouch technologies have been licensed by over 80 partners, including security and anti-virus vendors, managed service providers and messaging security providers.

Benefits of Anti Spam LIVE

Those who optimize IceWarp's *standard* antispam engine and tweak it to meet their business's distinct needs, can come close to 90% in spam identification. However, this requires time and sometimes coordination between the system administrator and end users.

Anti Spam LIVE profoundly improves spam management. Not only does accuracy reach beyond 98% accuracy, user activity is more secure and the time spent on spam administration is reduced.

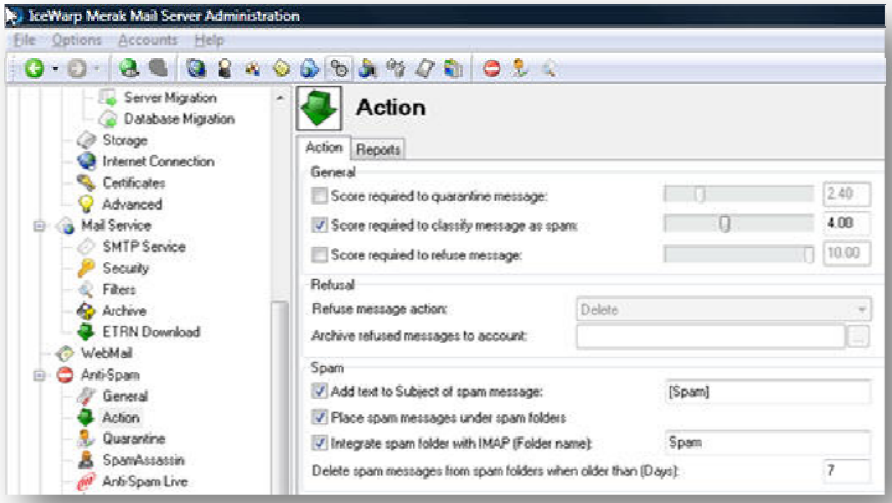
IceWarp Anti Spam LIVE will help protect servers and accounts from phishing attacks, adaptive spamming strategies, and malware sent from zombie botnets.

In order to provide high level real-time spam protection, Commtouch utilizes sophisticated proprietary technologies. Users will not need to wait for software or subscription updates, which are typically released well after a new internet threat arrives. Commtouch is far more progressive, using RDP (Recurrent Pattern Detection) technology in order to prevent and block spam threats shortly after an outbreak occurs.

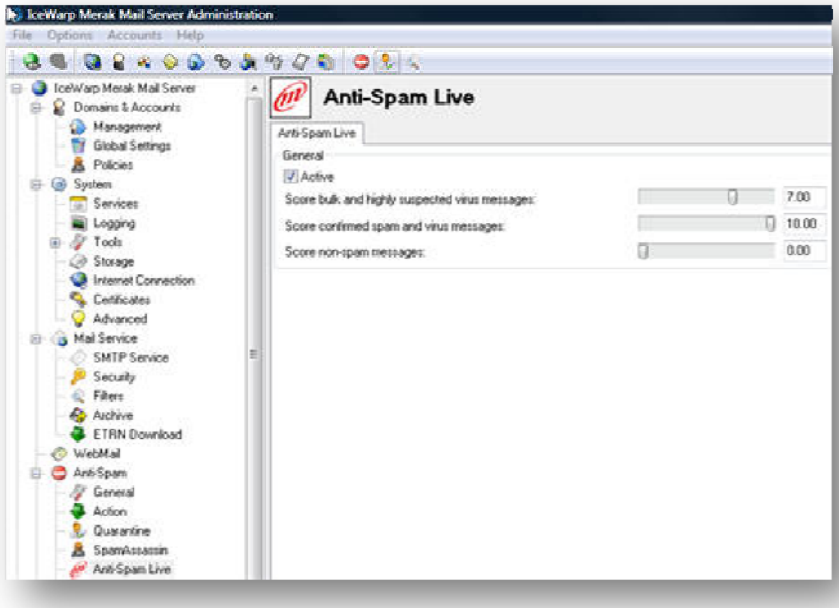
Configuring Anti Spam LIVE

To take advantage of the Anti Spam LIVE service, an administrator must first configure score settings in the standard Anti Spam engine. Remember, the scoring system determines spam identifying thresholds.

- The administrator must go to the [Anti-Spam], [Action] tab and specify the desired identifying score for the option, [Score required to classify as spam]. For instance, a message that falls beneath level 4 will be approved by the system if level 4 is the established threshold. Put another way, a message ranked as 4 or higher will be deemed as spam.



- Once the spam score is established in the standard Anti Spam engine, the administrator can use it to establish Anti Spam LIVE parameters.



- Messages determined to be part of a bulk delivery will be scored as spam.
- Messages potentially carrying a virus will be scored as spam.
- Messages originating from known spammer systems will be scored as spam.

- Since IceWarp Anti Spam LIVE is so reliable, IceWarp recommends that a high score setting be established. The rate of false positives is extremely low.

Anti Spam LIVE adds an additional layer of protection, identifying spam that has made it through the initial filters. If, however, a message is identified as spam by the initial filters, Anti Spam LIVE will not be summoned to perform a check, unless the administrator has used this option to score non-spam messages. This means that every message will be scanned by Anti Spam LIVE.

Afterword

When Anti Spam LIVE is configured to run in concert with IceWarp's standard antispam engine, spam identification reaches near perfection – a success rate of about 98 percent.

In addition:

- Time expenditure for email management will be reduced
- False positives will decrease, requiring less manual scrutiny of the spam folder
- Processing and server performance will increase as spam management becomes streamlined and more efficient
- Space required for mail storage will be decreased, often by half
- Greater efficiency in spam management means that the system administrator can tend to other infrastructure concerns