



2006 Email-borne Malware Review

Server-Side Polymorphic Viruses Defeat Traditional AV

January 10, 2007

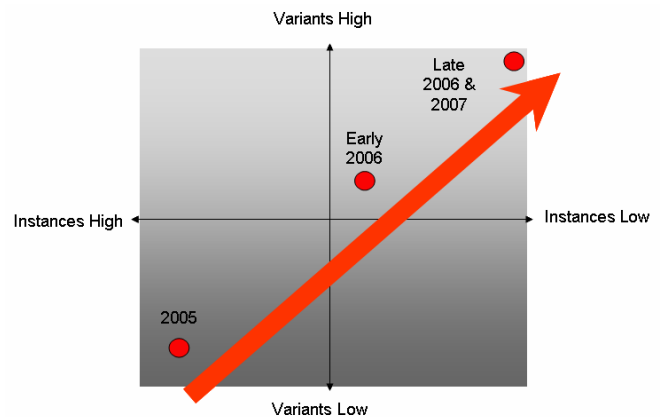
2006 was a year of fast-paced development for malware writers and fighters alike. Despite the anti-virus industry's heavy investments in narrowing the zero-hour gap, the emergence of a daunting new massive-variant distribution and infiltration method rendered those advancements ineffective. Massive-variant virus outbreak patterns have enabled viruses to carry out their malicious activity virtually unfettered by common anti-virus signatures and heuristics.

In 2006, malware writers adopted and developed a method of launching successive low-volume waves of distinct variants. This method is challenging because each new group of malware variants within the outbreak must be identified and blocked, separately. By constantly launching short-burst attacks of new variants, the malware writers always stay a step ahead of traditional AV solutions. No heuristic can block all of the variants and by the time a signature is released, that particular outbreak has ended, and several new variants have been released. By overwhelming the AV engines with variants, the outbreak remains a threat for weeks to months. In 2006 the massive-variant viruses turned every hour of an attack into a zero-hour.

Single-Variant, High-Volume Outbreak Patterns

Prior to 2006, most significant email-borne malware outbreaks focused on distributing high volumes of copies of the same malicious code, known as 'instances.' The intent was to infect as many computers as possible before a signature could be propagated to all AV subscribers. There was no pressure to update signatures too frequently; once a day was considered sufficient. A typical distribution pattern would generally begin with a gradual ramp-up in volume of instances. It would then continue at a

Email Borne Malware Trends 2005-2007



2006 Malware Highlights

Throughout 2006, malware transitioned from attacks of single-variants or a low number of variants with very high-volume, to outbreaks of massive numbers of variants, each in low volume.

Examples of the evolution of malware distribution techniques:

Single/Low-Variant, High-Volume

- Nyxem
- Sober

Overlapping-Variants, High-Volume

- Bagle
- Goldun
- Breplibot

Short-Waves, Low-Volume Variants

- Feebs
- Mytob
- Scano
- Lovegate
- Kukudro
- Stration/Warezov

Server-side Polymorphic

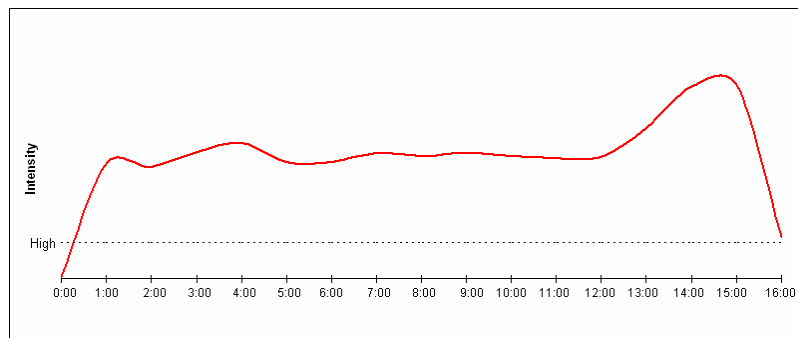
- Happy New Year!



high plateau that would last for hours to days. This plateau period would typically be comprised of successive blasts of the same code. For example, the **Nyxem** malware broke out in mid-January 2006 with a single variant that released several hundred instances of identical code every hour for nearly 24-hours.

A **Sober** malware outbreak that began in late 2005 is also a good example of this single-variant, high-volume outbreak pattern. Sober released tens to hundreds of thousands of instances each hour for 16 hours. A signature released by an AV vendor and updated by the client application within the first few hours of the outbreak would have protected users for the majority of the attack.

Typical Single-Variant High-Volume Outbreak Sober, November 2005



Source: Commtouch Labs

Overlapping-Variants, High-Volume Outbreak Patterns

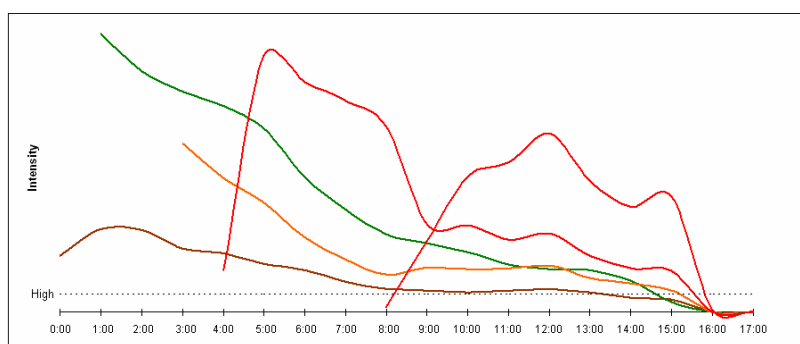
Occasionally, malware writers overlapped several high-volume variants within a single outbreak. In this type of outbreak, several slightly modified variants are launched at about the same time to increase the chances of penetrating defenses. A signature for one variant may be ineffective protection against the other variants. By the time new signatures for the other variants were generated and propagated, more machines would be infected by the same malware. A typical such high-volume overlapping-variant outbreak would last a day or two, some lasted as long as a week. A **Bagle** outbreak, seen in 2005, is shown above using this method.

Prior to 2006, the introduction of multiple overlapping variants was considered quite sophisticated, to the point that it was considered a newsworthy event.

Recurrent Low-Variant Outbreak Waves

Another technique used by malware writers in 2006 was to stagger the release of new distinct variants of the same malware over time, in short recurring waves. Release intervals can be any time period; days, weeks, even months. Since the new altered variants are distinct, the original signatures are ineffective against them, requiring the generation and propagation of new signatures. These new distinct variants of the same malware are

Typical Overlapping-Variant High-Volume Outbreak: Bagle, 2005



Source: Commtouch Labs

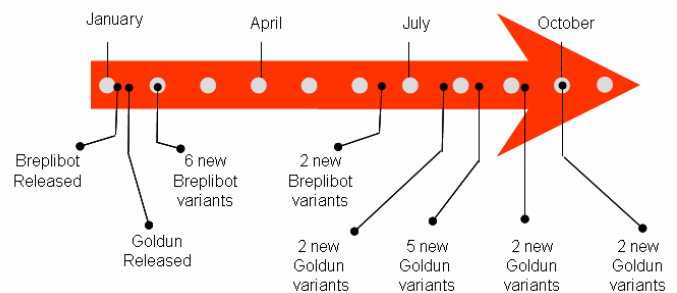


essentially new outbreaks from the perspective of AV engines. For example, in early 2006, the **Goldun** and **Breplibot** malwares were released in several distinct waves. These separate outbreak waves spread over a period of several months.

Blocking the Outbreak at Zero Hour

When outbreaks consisted of a single or few overlapping-variants with high-volumes, distributed for one or more days, it was effective to quickly detect and block the specific variants. Since releasing additional variants was not common, a signature developed at the beginning of an attack would maintain its efficacy for the remainder of the outbreak period. This approach, known as the 'zero-hour' method was highly effective, provided the anti-virus vendor was able to quickly produce a signature in the early stage of an outbreak. However, variant-by-variant signature generation and propagation is inherently too slow a process to be effective against high-variant malware. The erratic and unruly propagation process adds even greater difficulty.

Sample Recurrent Outbreak Waves: Breplibot and Goldun



Source: Commtouch Labs

During 2006, anti-virus vendors invested heavily in narrowing the zero-hour gap, and many added preemptive heuristics to their solutions. Their efforts paid off, and throughout 2006, leading anti-virus vendors significantly shortened their signature release cycles, on average providing protection within 10 hours of the outbreak. The limited amount of low-variant high-volume outbreaks could be blocked early enough to offer reasonable protection. However, such outbreaks became less common during 2006, as continuous, successive, low-volume variant outbreaks—which are more difficult for heuristics to detect—became increasingly common.

Successive, Short-Waves of Low-Volume Variants

2006 bore witness to an accelerated evolution of a new email-borne malware distribution method. The concept of releasing more than a few slightly-modified high-volume variants shifted malware writers' focus from volume of instances to volume of overlapping distinct variants. In doing so, each group of consecutive variants comprised a dense "mini-outbreak" within the overall malware outbreak. It became impossible to protect against all variants with a single broad signature or heuristic rule, because they often differ greatly. Moreover, the variants are released in low volumes of instances, making it difficult to detect, analyze and develop a new signature or heuristic rule in time to provide protection. This distribution method has prolonged the detection time for new variants. Short variant lifecycles of just a few hours rendered chasing after each new variant with signatures and broad heuristics ineffective.

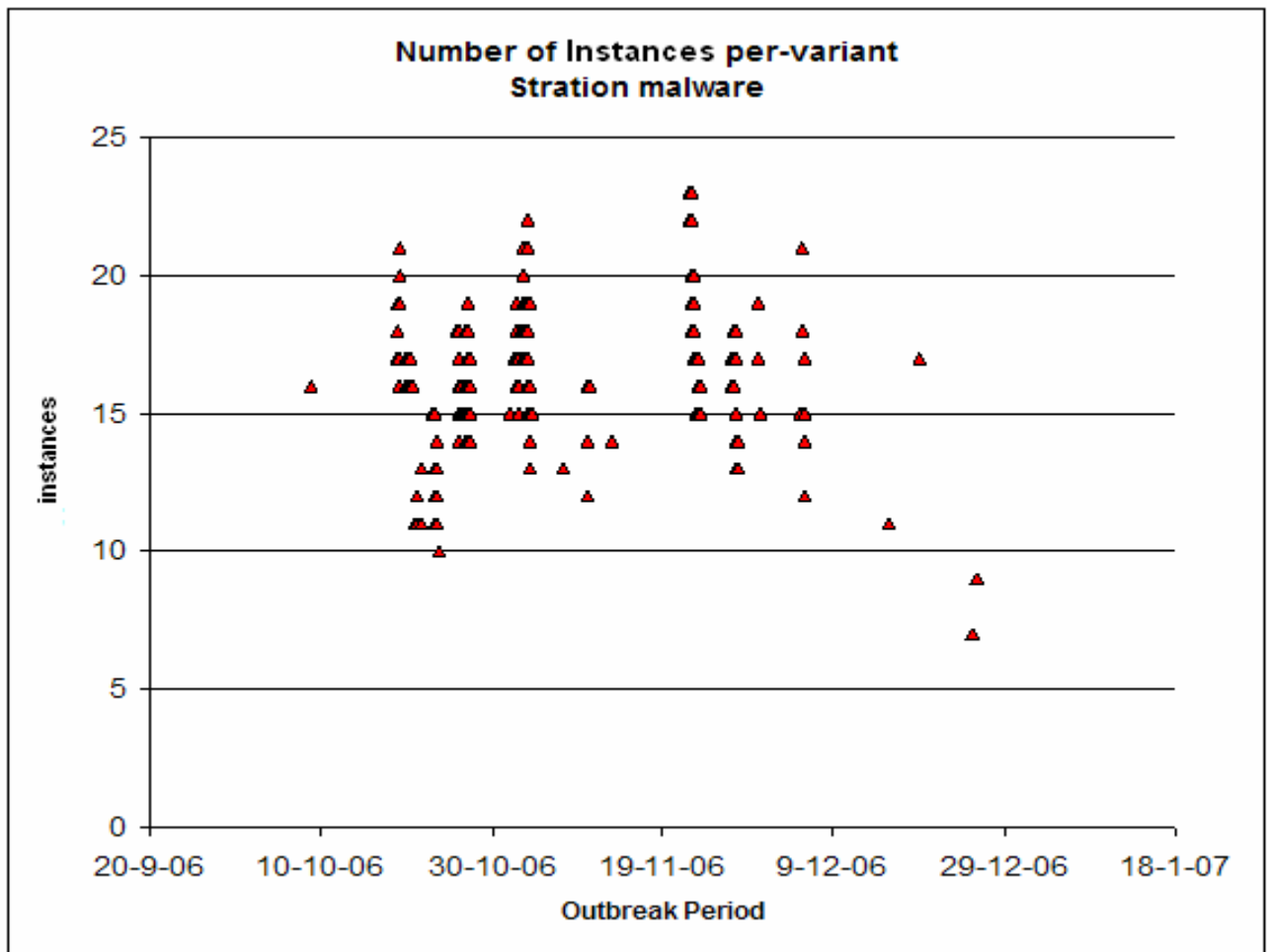
The new malware distribution method of successive, short-waves of low-volume variants gained considerable popularity by the end of the year. **Feebs**, **Mytob**, **Scano** and **Lovegate** are good examples of the gradual evolution of this new type of malware distribution throughout 2006. Another example is the Macro viruses in MS Office files that made a comeback in 2006, after nearly a decade of absence. These viruses suddenly cropped up in June in a burst of distinct variants that were delivered in multiple,



consecutive and overlapping waves. This malware family exploits the Macro script language found across Microsoft Office platform including: Word, PowerPoint and Excel. The outbreak, known by the moniker **Kukudro**, originated mostly in China and Taiwan, exploded suddenly across the Internet and flourished in several waves.

This trend of high number of variants with low-volume moved a step closer to server-side polymorphic viruses with the **Stration/Warezov** outbreak that appeared in July 2006, continued for over six months and shows no sign of ending. The chart below shows the release of distinct Stration/Warezov variants and number of instances over time. Each red triangle represents a distinct variant while the Y-value shows the volume of instances that Commtouch blocked in real-time.

Sample Short-Waves, Massive-Variant, Low-Volume Malware:
Stration, July 2006

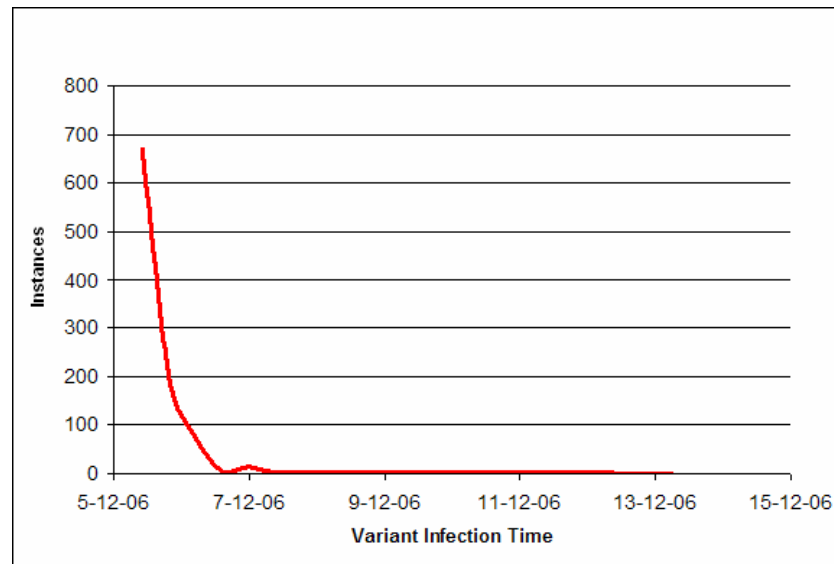


Source: Commtouch Labs

Taking a closer look at the lifecycle of a single Stration/Warezov variant (below) shows that the lifecycle is so short that, by the time a signature can be released, the attack is already over.



Single Variant of Stration Outbreak



Source: Commtouch Labs

The Dawn of Server-side Polymorphic Malware

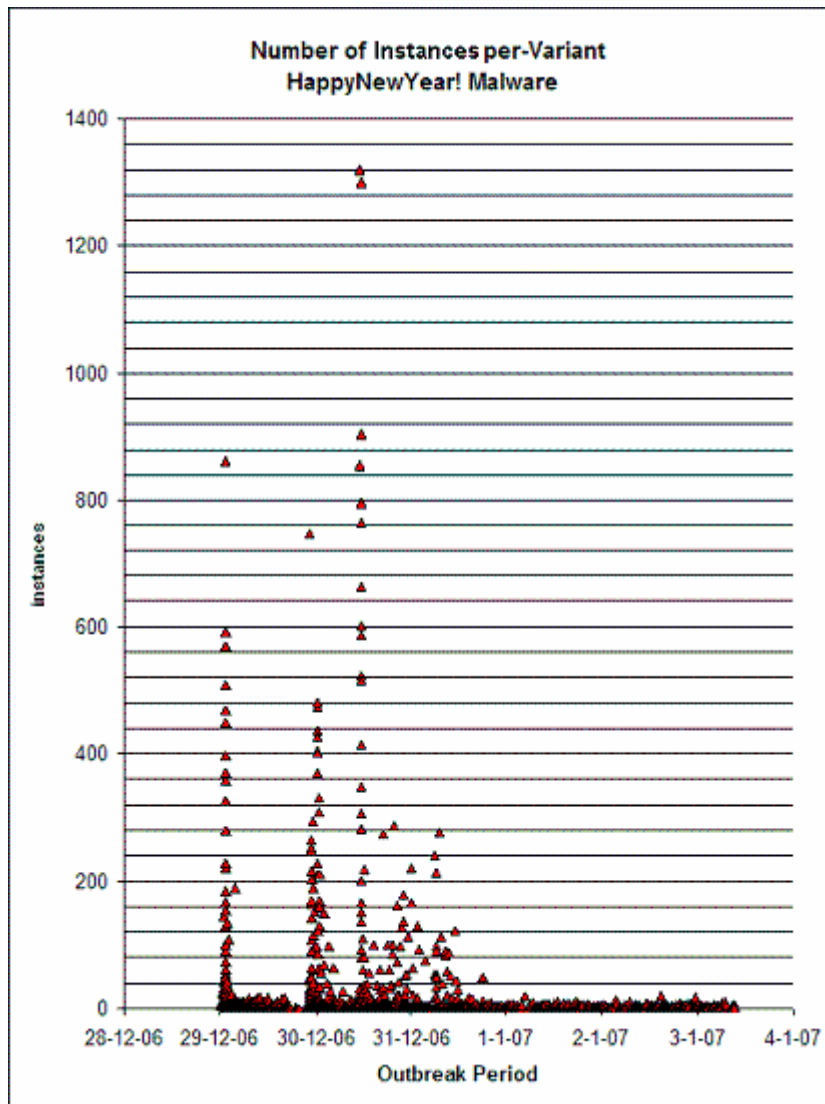
By the end of 2006, the new malware distribution trend had become even more formidable. In the last few days of the year, the **Happy New Year!** malware broke out with a simultaneous massive-variant outbreak so intense that it closely mimicked the behavior of the long-feared polymorphic virus. Happy New Year! is a server-side version of polymorphic malware, since instead of the code mutating 'on the fly' on infected machines, the malware writer generates a massive arsenal of unique permutations, then launches them all from multiple infection sources in quick succession..

Showcasing growing prowess, the massive malware infection broke out across the Internet simultaneously. Commtouch Labs' real-time detection intercepted some 3,262 distinct variants in the first 65 hours of the outbreak. Each variant contained a very small number of instances, distributed at an intensely rapid rate, from multiple infecting sources. The attack was so huge that during wave peaks it accounted for roughly 12% of all email traffic, worldwide.

The majority of the Happy New Year! variants, represented by red triangles for the six-day period depicted below, had between one and 50 instances each. Most of the distinct variants in the Happy New Year! outbreak were released at very short time intervals of just a few seconds to fragments of a second. During one five-minute period, Commtouch tracked nearly 850 distinct variants, suggesting that at the source the release interval was much shorter.



Server-Side Polymorphic Malware:
Happy New Year! December 2006

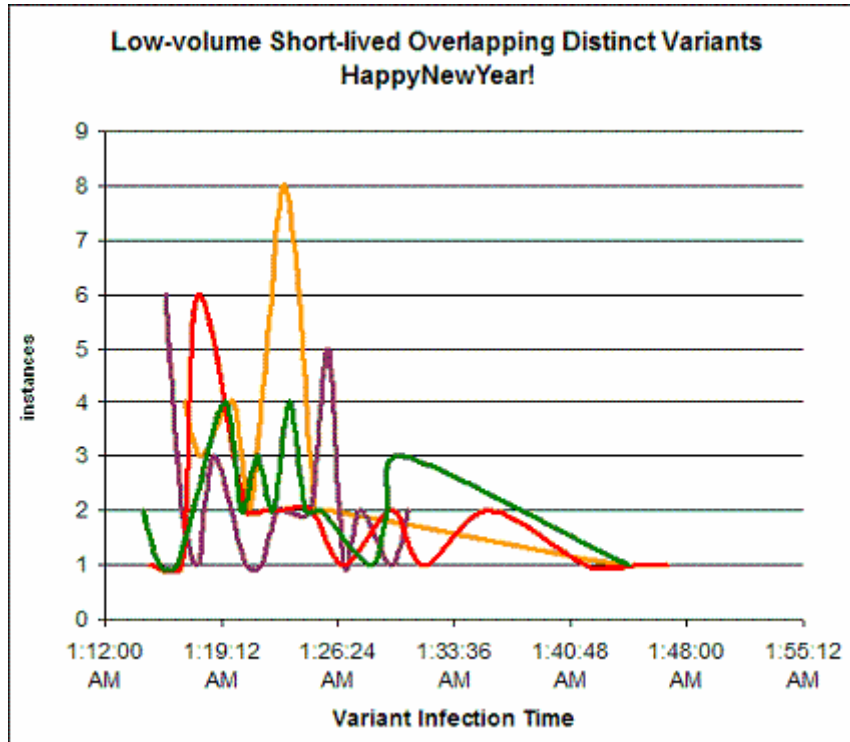


Source: Commtouch Labs

The graph below shows a selection of just four variants of the Happy New Year! malware, separated from a clutter of many additional overlapping variants. Malware variants are quickly moving targets. The collective variant attacks depicted below lasted less than two hours. By the time a leading vendor could propagate a signature, the simultaneous attacks were long over and multiple new variants were launched.



Selected Overlapping Variants of Happy New Year Outbreak: December 2006



Source: Commtouch Labs

Looking Ahead: Real-time Malware Outbreak Detection

2006 was marked by a gradual but clear transition from low-variant, high-volume outbreaks that could be contained within days, to fierce new massive-variant, low-volume outbreaks that continue to penetrate for week to months. This new method poses a formidable threat to even the most sophisticated heuristic and signature-based AV solutions. As malware distribution techniques approach server-side polymorphic behavior, the once appealing “zero-hour” doctrine of early protection has been rendered ineffective. In the face of massive-variant attacks launched in continuous waves of short bursts lasting for weeks to months, there is no longer a critical first hour of an outbreak: every hour is now a zero-hour.

Traditional anti-virus solutions have gotten faster at chasing down malware, but they have also trapped themselves in the paradigm of pursuit. In this scenario, the virus writers are always breaking ahead with new variants and AV solutions are perpetually chasing them. Commtouch chose a different approach to virus defense. Instead of focusing on hunting for new viruses and racing to catch them with a signature, Commtouch monitors billions of messages each week across the globe, in order to identify and block new malware outbreaks the very moment they emerge.

Commtouch Zero Hour Virus Outbreak Protection service delivers continuous real-time malware detection throughout massive-variant outbreaks. Based on patented Recurrent Pattern Detection (RPD™) technology, Commtouch identifies and blocks email-borne malware in real-time, providing immediate protection against new variants. As virus outbreak patterns continue to develop, real-time virus outbreak detection may prove the most effective response to coming challenges.



About Proofpoint

Proofpoint provides messaging security solutions for large enterprises to stop spam, protect against email viruses, ensure that outbound messages comply with both corporate policies and external regulations and prevent leaks of confidential information via email and other network protocols. The company's flagship products, the Proofpoint Messaging Security Gateway™ and Proofpoint Protection Server® provide future-proof messaging security using Proofpoint MLX™ technology, an advanced machine learning system developed by Proofpoint scientists and engineers. Proofpoint was founded by technology visionary and former CTO of Netscape Communications, Eric Hahn. The Cupertino, California-based company is funded by investors including Benchmark Capital, Bridgescale Partners, Inventures Group, JAFCO Ventures, Meritech Capital, Mohr, Davidow Ventures, and RRE Ventures. For more information, please visit <http://www.proofpoint.com>.

Proofpoint has integrated Commtouch Zero-Hour Virus Outbreak Protection technology as part of an optional module for its Proofpoint Messaging Security Gateway™ appliance and Proofpoint Protection Server™ software solutions to ensure advanced email defense for its enterprise clients. The Proofpoint Zero-Hour Anti-Virus™ module incorporates Commtouch Zero-Hour™ Virus Outbreak Protection to identify new virus activity and take preventive action at the earliest stages of a virus outbreak, keeping messaging systems safe until updated anti-virus signatures are available.

About Commtouch

Commtouch Software Ltd. (Nasdaq: CTCH) is dedicated to protecting and preserving the integrity of the world's most important communications tool -- email. Commtouch has over 16 years of experience developing messaging software and is a global developer and provider of proprietary anti-spam, Zero-Hour virus protection and IP Reputation solutions. Using core technologies including RPD (Recurrent Pattern Detection™), the Commtouch Detection Center analyzes billions of email messages per week to identify new spam and malware outbreaks within minutes of their introduction into the Internet. Integrated by more than 50 OEM partners, Commtouch technology protects thousands of organizations, with hundreds of millions of users in over 100 countries. Commtouch is headquartered in Netanya, Israel, and has a subsidiary in Mountain View, CA. For more information, see: www.commtouch.com, including the Commtouch online lab detailing spam statistics and charts.

Recurrent Pattern Detection, RPD and Zero-Hour are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.

Copyright © 2007