

## FEATURE 2

### VIRUS OUTBREAK PROTECTION: NETWORK-BASED DETECTION

Oren Drori

CommTouch Software, Israel

Timely response is the major challenge facing email security solutions. Today's malware is distributed more rapidly than ever before, with major outbreaks reaching their peak within a few hours. Unfortunately, while the response time of security software has improved over the years, there remains a dangerous window of vulnerability that can last hours or even days. Identifying new viruses, locking down signatures with 100 per cent certainty, and producing a vaccine is a lengthy process, leaving users unprotected while outbreaks are peaking.

This article suggests an alternative approach – pre-emptive mass outbreak detection – which represents a powerful complement to existing virus outbreak protection methods.

#### THE ACHILLES HEEL OF THE AV INDUSTRY

Despite heavy anti-virus investments, viruses and other types of malware are still the number one security problem facing computer systems. Reports suggest that malware damage exceeds \$55 billion annually.

The reason why malware attacks succeed is not that they are immune to vaccines. They succeed because they are fast and efficient enough to cause damage before users are vaccinated. Yet, despite the crucial importance of timing in the battle against malware, response time has not improved significantly for a number of years.

In recent years, the computing world has come to function as a global network – resulting in exponentially faster infection rates.

One of today's most significant drivers of virus production is spam. For spammers, viruses serve as an effective means of penetrating defences. This gives the AV industry a good deal to worry about, since it means that there is now a strong financial motivation to making viruses.

#### 'INNOCENT UNTIL PROVEN GUILTY'

The key factor determining the response time to new threats is the period between the outbreak's distribution and the moment protection is available on the desktop. Traditional anti-virus approaches are designed, first and foremost, to prevent 'false accusations': AV updates are released only after a bulletproof signature has been established. Even in the case of minor mutations, this process stretches over

hours. However, in the more severe case of a new virus type (the scenario with the highest probability of causing excessive damage) identification and vaccine creation can easily exceed 24 hours – a wide window of vulnerability.

Delays can happen for a number of reasons: lag time between distribution and first sample; lag time between first sample and signature; lag time between signature and production-level vaccination; and customer update schedule. Even if customers are updated several times per hour, several hours are lost before the first sample is identified and the first signature is created.

MyDoom is now considered the largest malware outbreak of 2004, and perhaps the one that created the most damage in the industry. The time of its release is unknown, but the peak occurred 6.5 hours after *MessageLab*'s first detection of the worm. Yet the first Beta signature, which came from *McAfee*, was released eight hours after detection – meaning that even the best-protected users were vulnerable during and after the peak. In fact, the first sample and general public protection were available 17 hours after first detection.

#### SIGNATURE-LESS TECHNOLOGY

As noted, anti-virus technology traditionally takes the 'innocent until proven guilty' approach. This means that messages are blocked only once they have been determined conclusively to be infected; until that happens, infected messages circulate freely.

Clearly, enormous end-user benefits are riding on the ability of the AV industry to minimize the vulnerability window, to provide what is called zero-hour or zero-day protection.

One highly promising new approach to zero-hour protection is real-time massive outbreak detection. This approach shifts the centre of gravity away from individual messages and towards the network itself. It is based on automated data collection and analysis, rather than manual intervention; and

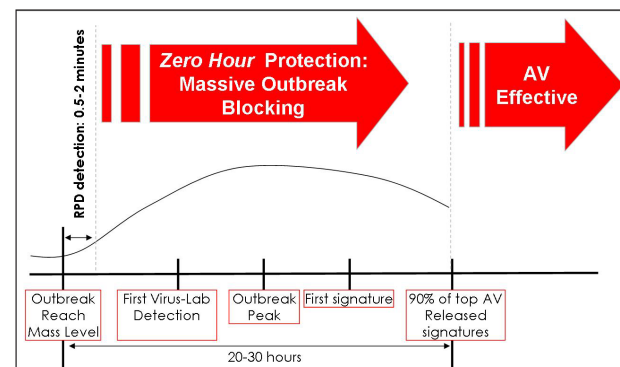


Figure 1: Outbreak detection plays preemptive protection role.

it risks delaying ‘innocent’ messages, rather than leaving users unprotected from emerging, unidentified threats.

Massive outbreak detection has already demonstrated detection rates of well over 95 per cent, coupled with extremely low false-positive rates. When used as an anti-spam tool – both by *Commtouch* and by big ISPs such as *Yahoo!* – it has years of immunity to the evolving obfuscation attempts of spammers.

### MASSIVE OUTBREAK DETECTION

Though implementation is far from simple, the technological concept behind massive outbreak detection is easy to understand. Very large amounts of real email traffic are analysed centrally, to identify recurrent distribution patterns. By identifying their mass-distribution patterns, it is possible to detect new email outbreaks within minutes, or even seconds, of their introduction into the Internet. Subsequently, each incoming message is compared, in real time, to an active outbreak database. Any message identified with a mass outbreak is blocked.

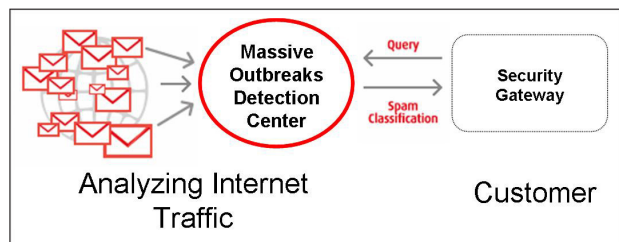


Figure 2: Commtouch's Recurrent Pattern Detection.

As mentioned, massive outbreak detection is far simpler in theory than in implementation. The first challenge in operating such a solution is obtaining real-time access to a live email stream. This stream must not only be of significant volume (millions or even tens of millions of messages), but it must also be a representative sample (geographic areas, etc.). Secondly, identification of recurrent patterns must be carried out automatically and with high efficiency.

Finally, this information must be communicated to the end user in real time, since using periodic updates would mean undermining the method's zero-hour capabilities. At the same time, communication with the end user must be highly efficient; clearly, an entire database of mass-outbreak indicators cannot be replicated for each end user.

### IMPLEMENTATION CONSIDERATIONS

Massive outbreak detection is a complement to existing anti-virus solutions, not a replacement. Its value can be summarized in two categories:

1. Early detection. Emerging outbreaks are identified ahead of time, and reported to the anti-virus labs. The lab can then determine if the outbreak is indeed a new virus, and respond accordingly.
2. Zero-hour prevention. Used as an additional layer in an anti-virus solution, massive outbreak detection provides valuable zero-hour protection. It buys precious time for anti-virus providers by blocking or detaining ‘suspect’ messages while the labs complete their analysis.

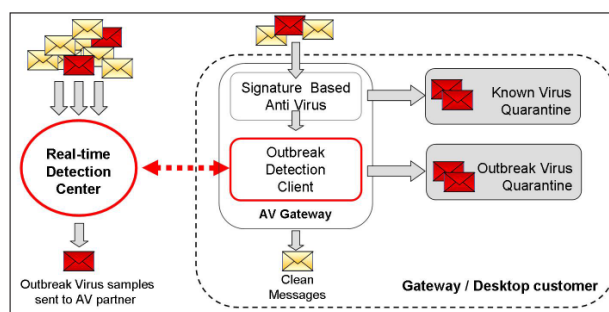


Figure 3: Mass outbreak detection complementing a traditional anti-virus solution.

### BUYING PRECIOUS TIME FOR AV VENDORS

Today's malware can spread at phenomenal speed, and the more networked our world becomes, the faster the infection rates are likely to become. Traditional anti-virus solutions experience difficulties in matching these infection rates, resulting in a window of vulnerability of strategic importance.

By identifying new outbreaks instantly and reporting them to the anti-virus labs, the massive outbreak detection technique can dramatically shorten the time to first sample. Needless to say, such time savings are critical.

By blocking instantly or at least detaining emails which are of mass-distribution nature, massive outbreak detection can prevent over 95 per cent of viruses from entering the user's inbox. This protection is available long before traditional AV signatures are produced.

This type of filter is nearly impossible to circumvent. It is effective against any type of threat that is mass distributed over the Internet – indeed massive outbreak detection is a mature technology, which has already been used widely to provide spam protection.

Massive outbreak detection is a signature-less network-based approach to email security, which provides a powerful ally to an anti-virus engine.