



White Paper

Preemptive Malware Protection through Outbreak Detection

Table of Contents

Executive Summary	.2
Response Time to New Outbreaks – The Achilles Heel of the Anti-Virus Industry	.3
Background	3
Malware-Distribution	3
Malware Protection	4
The "Innocent Until Proven Guilty" Approach	.4
Producing New Virus Signatures: A Lengthy Process	
The MyDoom Case Study: When Global Security Fails	.4
6:30 hours to the attack peak, 17:30 hours to global protection	.4
Outbreak Detection - A Preemptive Solution	.5
Automated Outbreak Detection: The Suspect-Profiling Approach	5
Recurrent Pattern Detection™ (RPD) - How It Works	6
Success Story — SoBig Worm Blocked by RPD, Hours Before the Anti-Virus Antidote	.6
Conclusion	.7

Table of Figures

Figure 1 — CSI / FBI Computer Crime Survey	3
Figure 2 — Data source: "Why your antivirus program won't catch the next attack" PC-Magazine, 06.08.04	4
Figure 3 — Outbreak Detection Plays Preemptive Protection Role	5
Figure 4 - Recurrent Pattern Detection	6

Executive Summary

Timely response has become the major challenge facing email security solutions

Today's Malware (malicious software – such as viruses, worms and Trojans) is distributed more rapidly than ever before, with major outbreaks reaching their peak within a few hours.

Unfortunately, the response time of security software has not improved significantly over the years, creating a dangerous window of vulnerability that can last hours or even days. Identifying new viruses, locking down signatures with 100% certainty, and producing a vaccine is a lengthy process, leaving users unprotected while outbreaks are peaking.

This white paper explains the inherent reasons for this vulnerability gap, and discusses how proactive outbreak detection can serve as a complementary early Malware protection method.

Response Time to New Outbreaks – The Achilles Heel of the Anti-Virus Industry

Background

Despite heavy investments in anti-virus (AV) solutions (99% percent of organizations use AV and 98% use firewalls), Malware is still the number one security problem facing computer systems.

Malware damage exceeds \$55 billion annually (Figure 1). According to a CSI/FBI 2004 survey, 78% of enterprises experienced at least one major virus attack during 2004.



Figure 1 — CSI / FBI Computer Crime Survey

Malware-Distribution

In the days when viruses were propagated by diskettes and file copying, infection rates were slow. In recent years, the computing world functions as a global network – resulting in exponentially faster infection (outbreak speed).

Another disturbing trend is that viruses are no longer just pranks. In many cases, they are produced and distributed by financially motivated professionals, who use highly advanced distribution technologies.

The reason why Malware attacks succeed is not that they are immune to vaccines. They succeed because they fast and efficient enough to cause damage before users are vaccinated. Despite the heavy price we pay for delays in response to new attacks, response time has not improved in any significant way for a number of years.

Malware Protection

The "Innocent Until Proven Guilty" Approach

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.

The traditional anti-virus approach is designed to prevent "false accusations" prior to any other consideration: Updates are distributed only when a bulletproof signature and means of defense are developed and successfully tested.

Even in 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.

Producing New Virus Signatures: A Lengthy Process

- Lag time between distribution and first sample: A good few hours may transpire from the moment a new virus is introduced to the time an anti-virus company becomes aware of it. AV companies are usually alerted to outbreaks by frustrated customers.
- Lag time between first sample to signature: This takes hours in the best scenario, and typically longer.
- Lag between signature and production-level vaccination: Once there is a solution for the virus it needs to be tested and documented. This may take days, if signatures do not suffice and AV engine modification is required.
- Updates are periodic: For example, Symantec's Live Update is only done once a week. IT managers conduct manual updates only in special circumstances.
- Virus Mutation and Proliferation: Handling mutations is an interminable task. Virus code is open or can be easily hacked and modified so it will be unrecognizable at the AV lab. It is then distributed again as a new virus requiring a new update.

The MyDoom Case Study: When Global Security Fails

6:30 hours to the attack peak, 17:30 hours to global protection

MyDoom is now considered the largest Malware outbreak of 2004, and perhaps the one which created the most damage in the industry:

- The accurate time of distribution is unknown
- MessageLabs was the first to detect the new virus (worm) in the wild (hour zero)
- 6.5 hours after the first detection, the outbreak had reached its peak (in terms of infection rate)
- Nearly 8 hours from first detection, the first signature was released Beta signature, by McAfee
- It took over 17 hours until the general public was protected (release of production-level signatures by 90% of the top 15 AV vendors)





so quickly that signature-based anti-virus protection is useless." META-group

"Worms propagate

MyDoom, The largest malicious outbreak in 2004 has reached its peak, before suitable signature was available by **any** of the leading AV-labs

White Paper

Outbreak Detection - A Preemptive Solution

Automated Outbreak Detection: The Suspect-Profiling Approach

As noted, anti-virus technology traditionally takes the "innocent until proven guilty" approach – allowing suspects to circulate freely rather than taking the risk of falsely detaining an innocent bystander. In security terms, this means that messages are blocked only once they are conclusively determined to be infected; until that happens, infected messages circulate freely, slowing down response times almost to the point of making the response altogether irrelevant. Clearly, the industry needs a response that can detect viruses faster, closing this large window of vulnerability.

Recurrent Pattern Detection (RPD[™]) technology was developed by Commtouch precisely for this function. Used as a complementary preemptive measure RPD can block new viruses hours before time-consuming signatures are available.

RPD identifies emerging Malware according to the outbreak patterns of typical attacks, particularly the more noxious ones. Suspect messages are held or delayed, much like a suspicious traveler might be detained at an airport in the post 9/11 era. Arrest requires hard evidence, but airport security can take immediate short-term action based on passenger profiling.

Similarly, by detecting messages that belong to mass outbreaks, RPD can proactively stop most viruses long before the full cycle of vaccination, testing and production is completed. (See figure 3)



Figure 3 — Outbreak Detection Plays Preemptive Protection Role

Recurrent Pattern Detection[™] (RPD) - How It Works

RPD is a proprietary, patent pending technology developed by Commtouch for detecting Malware based on its outbreak distribution pattern.



Figure 4 - Recurrent Pattern Detection

The Commtouch Detection Center analyzes massive amounts of real e-mail traffic over the Internet. By identifying recurrent patterns, it detects massive email outbreaks within minutes or even seconds of their mass distribution over the Internet.

RPD addresses a fundamental aspect of Malware: mass distribution patterns – rather than the individual message's content. This is a key factor underlying RPD's effectiveness and accuracy:

- Over 95% detection rate of any outbreak including unknown viruses
- Near zero (under 0.0004%) false positive rates (Osterman Research, October 2004)
- Quickest approach to respond against new outbreaks (IDC, April 2004).
- Content agnostic cannot be easily circumvent by spammers and hackers
- Extremely low false positives does not 'make guesses', only blocks or delays messages which belong to a massive outbreak.
- Fully effective against spam and Malware in any language, or file format.

Success Story — SoBig Worm Blocked by RPD, Hours Before the First Anti-Virus Antidote is Released

Quest Technology Management has been serving Fortune 50-5000 corporations, government and education since 1982. During the SoBig outbreak in August 2003, Quest found that the RPD-based solution they had implemented to block spam was doing much more than that: it was successfully detecting and blocking the SoBig worm from spreading throughout the enterprise and infecting customers.

The intervention of the Commtouch solution gave antivirus providers the time needed to develop effective antidotes. It prevented major inconveniences for Quest and its customers.

"It's a great relief to our customers that Commtouch Anti-Spam can act as a barrier against further spread of the SoBig worm from inside their organizations until they are able to deploy specific detection and removal capabilities from their anti-virus provider. When a virus writer uses spamming techniques, response time is critical, and we're pleased to be able to provide this additional layer of protection to our customers." Tim Burke, CEO, Quest Technology Management.

"When a virus writer uses spamming techniques, response time is critical, and we're pleased to be able to provide this additional layer of protection to our customers."

> Tim Burke, CEO Quest Technology

Conclusion

Today's Malware can spread at phenomenal speed; and the more networked our world becomes, the faster the infection rate is likely to be. Traditional anti-virus solutions cannot match these infection rates, because they require hours or even days to launch a specific vaccine for each new threat. Before a new virus is detected, before a signature is found, before a vaccine is developed, tested and distributed – we find that the virus has already infected millions of users and caused untold damage.

Closing this wide window of vulnerability requires a more proactive approach to Malware, capable of protecting users from the first moments of each new attack.

Outbreak-based protection is a powerful complement to existing signature-based approaches, offering the automatic proactive protection the industry needs. By focusing on the typical distribution pattern of Malware attacks, this approach effectively detects emerging outbreaks in the first few seconds or minutes. From that moment, each message associated with the Malware outbreak is identified – providing the timely proactive protection users need.

Commtouch Inc. Ltd.	Commtouch Software
1300 Crittenden Lane,	1A Hatzoran St
Suite # 103,	P.O. Box 8511
Mountain View, CA 94043. USA	Netanya 42504, Israel
Tel: +1 650.864.2000	Tel: +972-9-863-6888
Fax: +1 650.864.2002	Fax: +972-9-863-6863

© Copyright Commtouch Software Ltd. 1991-2004 All Rights Reserved.

The information contained in this document is subject to change without notice. Commtouch makes no warranty of any kind. Commtouch will not be liable for any direct, indirect, incidental, consequential or other damage alleged in connection With the furnishing or use of t his information. Except as allowed by copyright laws or herein, reproduction, adaptation, or translation without prior written permission is prohibited

RPD™ is a registered trademark of Commtouch Software Ltd. All other trademarks rights, that may be referenced and/or mentioned in this document, belong and are registered by their respective owners.