

# Defending networks against rapidly evolving threats

A Sophos positioning paper

March 2006

The challenge for organizations today is to stay ahead of the increasingly interconnected threat from rapidly spreading and evolving viruses and spam campaigns, phishing scams, spyware, and other threats. This paper describes how the expertise and systems in SophosLabs™ give businesses the rapid and reliable protection they need to ensure business continuity. It describes how, by analyzing the “genetic” make-up of programs and messages, Sophos’s Genotype™ technology provides preemptive protection from emerging viruses and spam campaigns.

## The accelerating pace of change

Malicious threats such as viruses and spam campaigns now evolve rapidly, often using a combination of methods to spread. Typically, when a new malware threat or spam campaign appears, security vendors react by quickly creating specific virus detection algorithms and new anti-spam updates which detect and counter the threat. In response, virus writers release new viruses as frequently as possible, often distributing multiple strains of the same threat in a short space of time, in order to increase the chances of survival of their creations. Similarly, spammers use a variety of tricks to circumvent specific anti-spam technologies and rapidly adapt their campaigns to beat the filters.

In this continuously evolving threat environment, financial motivation has driven virus writers and spammers to join forces to produce campaigns that coordinate virus, spam, phishing, and spyware attacks. The random vandalism of earlier generations has been replaced by more purposeful criminal activity, with a shift in emphasis away from “traditional” viruses towards threats designed to steal money, information, or both. Trojans and other spyware such as keyloggers now form the majority of new threats analyzed by SophosLabs™ – a global network of threat analysis centers.

## Winning with technology and expertise

As a response to the evolution of threats, a number of standalone “day zero” solutions have emerged. However, effective protection requires a combination of the rapid creation of new virus and spam identities, and preemptive generic detection. An integrated approach is also important – using multiple vendors to protect different parts of a network introduces vulnerability gaps, since the distinction between different types of threat is not always clear. Bofra, for example, was a threat which not only exploited an internet browser vulnerability in order to spread, but also shared some characteristics with spam and viruses, attacking through both the gateway and endpoint. The interconnected technology and

pooled expertise in SophosLabs enable its highly skilled experts to respond rapidly and effectively to emerging threats, no matter what combination of techniques they use to spread.

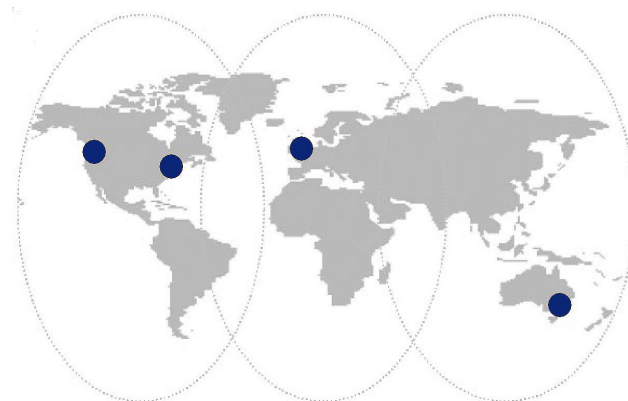


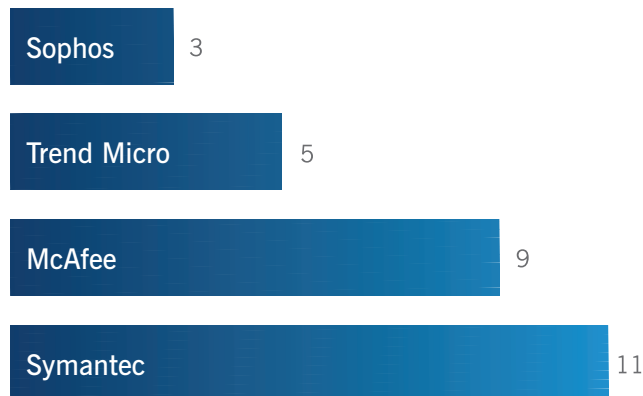
Figure 1: SophosLabs – providing 24-hour analysis and protection

New threats tend to shadow the working day; that is, they follow the sun from Asia across Europe and Africa and on to the Americas. The strategic positioning of SophosLabs in Asia-Pacific, Europe and the east and west coasts of North America, as shown in Figure 1, means that these centers can have updated protection created and deployed before the working day even begins in many regions.

SophosLabs analyzes tens of thousands of files a month for viruses and millions of emails each day to determine whether they are spam. Sophos uses automated systems, such as Mentor, which replicates and analyzes viruses, to accelerate the production of new anti-virus updates. A database holding threat information from Sophos’s 20 years’ experience in combating threats makes a wealth of data available to the labs’ analysts



worldwide. New anti-spam updates are created and deployed several times an hour. This response to new spam attacks is complemented by the fastest response times of the major security vendors to new virus outbreaks, as shown in Figure 2 below.



Average response times (hours)\*

Figure 2: Average response times to new threats in 2005

Through its rare combination of cross-threat expertise and powerful integrated technologies, SophosLabs is uniquely placed to provide consolidated protection to combat the increasing sophistication of the new breed of cybercriminals. The global visibility which SophosLabs has of emerging threats also enables Sophos to provide additional alert services. Sophos ZombieAlert™ Service provides organizations with immediate warning if spammers have hijacked any of their computers to send spam or launch denial of service attacks. Sophos PhishAlert™ Service, meanwhile, provides alerts of phishing campaigns, so that targeted organizations can take steps to shut down any fake websites which have been set up in order to steal from their customers.

### Cool technologies, red hot protection

SophosLabs is able to provide rapid protection through the experience and intelligence of its experts and through its range of highly refined technologies and detection methods. These factors combine to protect businesses against existing and emerging threats, no matter how complex the method of spreading. Viruses, spyware, Trojans, and worms are detected using a combination of techniques that include:

- Dynamic Code Analysis™ – a range of techniques used by the Sophos virus detection engine, and in particular the technique for detecting more complex encrypted malware.
- Algorithmic pattern-matching – input data is checked against a set of known sequences of code already identified as a virus.

- Emulation – a technique for detecting polymorphic viruses, i.e. viruses that hide by encrypting themselves differently each time they spread.
- Threat reduction technology – the detection of likely threats by a variety of criteria, such as double extensions (for example .jpg.txt) or the extension not matching the true file type (e.g. an executable or .exe file with the extension .txt).

Spam is blocked using methods that include:

- Content scanning – cleaning up and deconstructing complex, disguised messages.
- Obfuscation detection – catching common techniques used to disguise spam content, such as substituting letters for numbers, e.g. V1agra.
- Sender reputation filtering – cross-referencing the sender's IP address against the Sophos IP Block List, a list of known spammer IP addresses.
- Call to action/URI analysis – examining calls to action in emails, for example looking for known spammers' phone numbers and instant messaging IDs, as well as spammer websites and domains.
- Spam identities – using content-based checksums generated from captured spam to detect messages from known spam campaigns.
- Heuristics – using carefully constructed heuristic rules to search in multiple languages for known spam constructions within the content of emails.
- Automated tuning – adjusting the weighting of tests to catch campaigns designed to bypass a single, popular filtering technique.

### Unraveling the helix

All these methods put Sophos protection at the top of the league in terms of speed and reliability. In addition, Sophos Genotype technology – which is used in Sophos's endpoint and gateway solutions to deliver protection at the desktop, laptop, server and gateway – allows us to protect businesses at an even earlier stage by delivering preemptive generic protection against threats before they emerge. Genotype technology is incorporated in the Sophos virus detection engine and anti-spam engine. It focuses on detecting new variants of

---

*Genotype technology stops new threats before specific detection is available and even before Sophos has the sample to analyze.*

---

existing families of spam campaigns and viruses. It has its analogy in the world of living organisms. In biology, the genotype is the genetic make-up of an individual organism. It is composed of genes, i.e. segments of a DNA molecule, which are units of information inherited from parent organisms. Sophos's Genotype technology looks at the "hereditary information" in new viruses or spam messages and detects when the threat is a close relative of one which is already known.

### ***Sophos Genotype virus detection***

Virus writers regularly reuse the majority of an original virus's code – there are, for example, thousands of variants of the Rbot virus. Even if new malicious functionality has been added, the new virus remains similar to the original threat and is part of the same family. It is this similarity that Genotype technology exploits, by extracting the complete genotype of a program. Genotype technology avoids the false positive problem common in conventional heuristic detection by targeting specific virus and spam families.

---

*Sophos Genotype virus detection technology extracts a program's genotype and tries to match it against the genotype of existing viruses.*

---

Every program has its own genotype. However, the genotype of a malicious program, such as a virus, significantly differs from the genotype of a non-malicious program. In addition, genotypes of a particular virus family differ from the genotypes of another virus family.

Some examples of genes which may be found in a malicious program are:

- the ability to copy itself to the system folder
- the ability to spread using vulnerabilities in the operating system
- the ability to change registry keys so that it starts automatically when the user logs on
- the ability to search the local hard drive for email addresses
- the ability to send itself as an attachment of an email message.

---

#### ***Examples of Genotype success***

- *100% detection of Aribot variants*
  - *100% detection of Baba variants*
- 

Extracted genes are matched with genotypes of all known families of threat using a finely tuned scoring system. When the genotype of the examined file matches the genotype of a known family of viruses, Sophos Anti-Virus reports the virus as a genotype (e.g. W32/Rbot-Gen).

### ***Sophos Genotype spam detection***

Spammers constantly introduce new techniques in an attempt to succeed. By sending spam through "fresh" open proxies, they try to prevent their messages being blocked by IP-based block lists. To bypass reputation filtering, spammers register hundreds of new domains for each spam campaign, making them harder for security vendors to react to. By randomizing obfuscation patterns, rotating phrases, and adding random unrelated words and phrases, spammers can ensure that every recipient gets a message that looks different from the other ones in the same campaign. These techniques impact the efficiency of spam detection signatures and basic content analysis.

Spammers also use randomization in images so that they are not identical to others in the same spam campaign. This can be done by changing just a few pixels, so that the image will still appear the same to recipients. Some spam emails (for example stock market scams) often contain no call to action in the message, which makes call to action and URI analysis less effective.

Nevertheless, spam can still be detected and blocked. All messages within a given spam campaign have a number of common attributes that stay the same – for example, the message size range or the presence of certain email headers and their attributes. For each campaign, experts in SophosLabs create a unique genetic spam campaign template that can be applied against incoming message traffic.

---

*Sophos Genotype spam detection technology creates a genetic spam campaign template by identifying static and changeable campaign genes.*

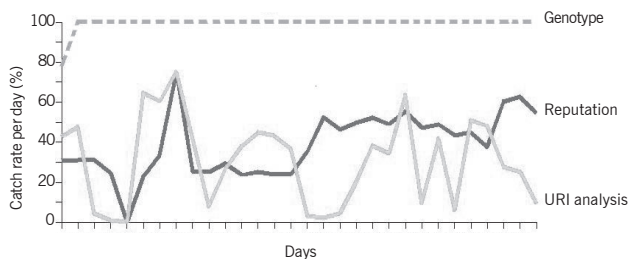
---

Examples of what a template will check for are:

- Does the URL found in this message end with a .aspx string followed by a question mark and 5 to 7 digits?
- Does the HTML part contain a table with three rows on a pink background?

Messages that match the template are identified as a known spam campaign and will be blocked automatically as spam. Some genotype definitions are short-lived and are created to address a specific spam outbreak, while others that address long-running spam campaigns might stay active for a long time. With other anti-spam techniques by themselves blocking

up to 95% of all spam traffic, Genotype technology is used only where conventional anti-spam techniques are less efficient or do not work. However, its value in protecting networks is significant, as Figure 3 shows. The graph shows the effectiveness of Genotype detection in one email campaign over one month – a single Genotype definition has been catching 100% of the messages almost every day. The graph shows the difference in catch rates for the campaign using Genotype technology, URI analysis, and reputation filtering.



**Figure 3: Genotype technology, reputation filtering, and URI analysis compared over 30 days**

Sophos analysis shows that, even though genotypes block only about 5% of all spam, they provide 100% protection against the spam campaigns that are harder to detect with solutions using just reputation filtering and anti-spam heuristic rules. Genotype technology provides unique proactive detection against the latest mutations of a campaign.

## Conclusion

Through a powerful combination of expertise, technology, and global visibility of emerging threats, SophosLabs provides the 24/7 research and rapid global response businesses need to protect them from increasingly complex threats. “Day zero” protection through Genotype technology integrates with a range of other highly tuned techniques and technologies to provide Sophos users with a level of protection that others can only dream of.

*To find out more about Sophos and how our products can protect your organization, visit [www.sophos.com](http://www.sophos.com).*

## About Sophos

Sophos is the world leader in integrated threat management solutions purpose-built for business, education and government. Our reliably engineered, easy-to-operate products protect over 35 million users in over 150 countries. Through 20 years’ experience, combined in-house anti-virus and anti-spam expertise, and a global network of threat analysis centers, we respond rapidly to emerging threats – no matter how complex – and achieve the highest levels of customer satisfaction in the industry.

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France  
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

© Copyright 2006. Sophos Plc.

*All registered trademarks and copyrights are understood and recognized by Sophos.  
No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
WWW.SOPHOS.COM