SOPHOS

Protecting against tomorrow's threats today – proactive security from SophosLabs

Constantly looking for new vulnerabilities to exploit, today's cybercriminals are using fast-changing, low-profile threats to surreptitiously infect and hijack computers across the business network. Spammed email, infected endpoint devices and above all the largely unprotected web, are all part of the rapidly evolving threat landscape in which an increasingly mobile workforce presents unprecedented challenges to business security and productivity.

This paper describes how, through the powerful integration of cross-threat expertise, automated systems and leading-edge technology, SophosLabs has the global visibility and 24/7 research operation to provide the proactive protection and rapid response that businesses need to safeguard their security, productivity and regulatory compliance.

A Sophos positioning paper

February 2008

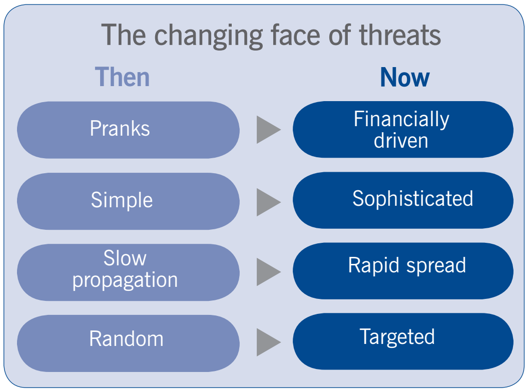
Protecting against tomorrow's threats today – proactive security from SophosLabs

The changing nature of threats

Virus and spyware writers, spammers and phishers continue to collaborate to create complex, blended threats. These threats are increasingly surreptitious and low profile, mutating in hours or even minutes to evade detection.

The web has displaced email as the hacker's main vector of attack, with malicious code being embedded in high-traffic websites or banner ads. In 2007, Sophos discovered a newly infected webpage every 14 seconds[1]. As the lines between the different types of threat have become blurred, it no longer matters where they come from – web download, email attachment, endpoint device, or guest laptop.

Alongside more traditional threats, potentially unwanted applications (PUAs) like adware, dialers and hacking tools, can also pose severe security issues and usually have no place on a business network. The uncontrolled use of legitimate technologies, such as Voice over IP (VoIP) and Instant Messaging (IM), as well as social networking websites, presents further challenges, impacting productivity by consuming network bandwidth and employee time.



The changing face of threats

Then	Now
Pranks	Financially driven
Simple	Sophisticated
Slow propagation	Rapid spread
Random	Targeted

Inside

The changing nature of the network

At the same time, today's working environment is rapidly changing. The network perimeter has dissolved to such an extent that it is virtually unidentifiable. Yesterday's "castle and moat" architecture – with its office-based desktops and servers protected by a gateway firewall – has crumbled. Remote working, the use of endpoint devices such as USB sticks, constant internet access and the rapid emergence of Web 2.0 technologies have redefined how employees interact with an organization's systems. In addition, increasingly complex networks must accommodate not just employees, but also outside contractors, vendors and customers.

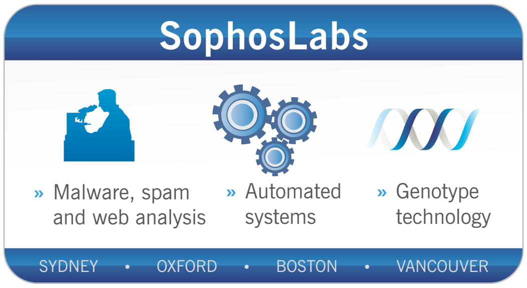
The global strength of SophosLabs

It is within this increasingly challenging environment, in which rapidly evolving blended threats relentlessly attempt to breach an ill-defined perimeter, that SophosLabs™ operates.

The response of the security industry to this environment has been to move away from point solutions to more consolidated products. However, using protection from vendors who have simply acquired spam and web capabilities, but have not integrated their expertise, analysis and technologies, produces vulnerability gaps – in much the same way that using multiple vendors to protect different parts of the network does.

It is in its unique approach to closing these gaps that SophosLabs' formidable strength lies. Its exceptional visibility of web threats, spam, malware and unwanted applications is matched by cross-threat expertise, highly tuned proactive systems, and powerful integrated technologies. Its ability to provide round-the-clock protection at every point on the network is underpinned by global insight from a broad base of data sources that include:

- Spam traps in over 50 countries, providing instant visibility of new spam campaigns
- Global email traffic from thousands of customer deployments
- Third-party resources that report and share threat information
- Data-sharing partnerships with search engines
- Millions of daily feeds of malicious URLs.


SophosLabs
» Malware, spam and web analysis
» Automated systems
» Genotype technology
SYDNEY • OXFORD • BOSTON • VANCOUVER

Placed strategically around the world, SophosLabs' integrated network of labs shadows the working day, providing follow-the-sun analysis and protection. As one lab closes for the night, the next takes over: Sydney>Oxford>Boston>Vancouver>Sydney. Each lab in the network is capable of detecting, analyzing and publishing protection against the full range of security threats: viruses, spyware, spam, unwanted applications and malicious URLs.

While some approaches require large numbers of people to process and respond to emerging threat data, SophosLabs uses a smaller team of experts and highly advanced, proactive automated systems. In combination, they dissect tens of thousands of files for malware every month and analyze millions of emails and webpages every day, allowing them to block thousands of malicious URLs. Each lab can deploy protection directly to the customer in seconds, blocking malicious code even before it executes.

Integrated expertise, protecting every point

Just why an integrated approach is so important can be seen in the Storm worm (also known as "Dorf" and "Dref"), which first appeared in August 2006. It evolved so rapidly that it spawned more than 5,000 variants in just eight months (see figure 1) and saw over 50,000 variants in 2007 altogether.[2]

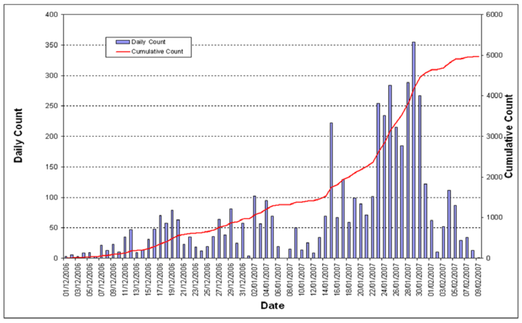


Figure 1: Storm – 5,000 variants in eight months

Storm arrived as waves of malicious emails with a variety of subject lines from breaking news stories to ecard greetings. One variant, claiming to point to a YouTube video, urges recipients to click on a link to download the video.

In fact, the link sends them to a webpage containing a malicious script and a Trojan designed to compromise their computer and turn it into a zombie. Once a computer is under outside control, more malware and junk mail can be spammed out or distributed denial-of-service attacks launched. Because Sophos has the expertise to identify and block malicious websites, spam and malware, the web, email and endpoint are all rapidly and automatically protected.

> *Sophos detection technology is used in 30% of all available security appliances and is the power behind the offerings of more than seventy-five other security vendors, including OEMs, managed service providers, and strategic alliance partners.*

High-capacity, automated analysis

Instead of using an ever-growing number of people, SophosLabs uses an extensive and constantly evolving set of tools to detect and analyze malware and its sources. Its worldwide analysts are also able to call on a database that holds threat information gathered during Sophos's 20 years' experience.

Backing up this database are two key systems:

- Mentor – an automated system that emulates and analyzes viruses and malware and which accelerates the production of new anti-virus updates
- Genie – a massive database containing terabytes of data that identifies malicious and suspicious behavior data. Genie enables quicker detection of – and proactive protection against – new and evolving threats, and underpins Sophos Genotype® Technology (described in the next section).

SophosLabs' cross-threat expertise: example scenario

- A malicious spam email arrives at a Sophos spam trap, linking to a malicious webpage, such as a fake ecard greeting
- SophosLabs analyzes the email, following the URL link to a drive-by downloadable Trojan
- SophosLabs extracts the spam identities and URL, and:
  - adds the information to its anti-spam detection data
  - adds the URL to its web-threat database
  - adds the Trojan to its virus database
- The characteristics of the malware are extracted and used to create proactive protection
- Updated protection is automatically deployed to all Sophos customers at each of the stages
- SophosLabs continues to monitor the webpage for new variations of the threat and automatically adds protection for any that are found.

Proactive protection: Sophos Genotype Technology

Key among the technologies used by SophosLabs is Sophos Genotype Technology which is incorporated in all Sophos's web, email and endpoint security and control products.

Traditionally, protection against malware and spam was created by security vendors collecting samples of particular viruses and spam, and then developing specific signatures. Today this method is simply too slow and inadequate – there are too many targeted threats and they mutate too rapidly. The only answer against these new "zero-day" threats is to stop them pre-emptively and this is precisely what Sophos Genotype Technology does.

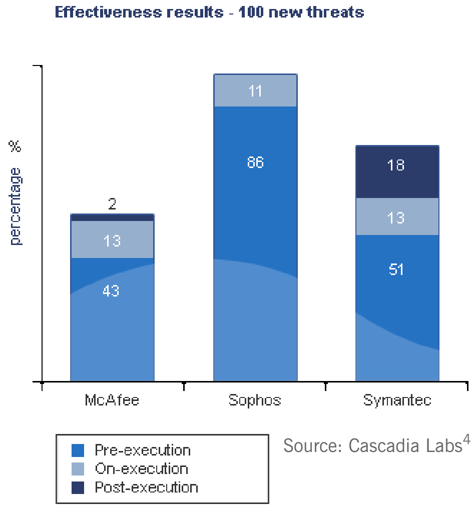
Independent tests from av-test.org[3] and Cascadia Labs[4] (see figure 2) have shown that Sophos Genotype Technology is the leading protection technology in the industry. It identifies malware or spam – even where the particular sample has never been seen before – by recognizing and extracting "genes" (or components of behavior). It then identifies the combinations of these genes (genotypes) that distinguish malware and spam from legitimate applications and messages. Extracted genes are combined to create a genotype using a finely tuned scoring system. By identifying genes from all the malware it has ever collected, SophosLabs can identify the characteristics and combinations of genes that appear in malware. It compares this information with data about the genes that are seen in known good files and, in this way, minimizes the risk of incorrectly identifying a file as malicious when it is not.

Sophos has combined Genotype Technology with other technologies designed to remove the administrative burden, ensuring that users get excellent proactive detection without the requirement of other approaches for administrators to modify detection by setting up their own rules.

Proactive malware detection

Sophos Genotype Technology:

- Protects against unknown or zero-day malware, including variants of known threat families
- Extracts and analyzes genes, comparing against known bad genes, known bad content and bad behavior
- Uses pre-execution analysis to detect threats without letting the code run, avoiding the risk of partial infection
  and damage
- Uniquely provides pre-execution protection at the email and web gateway, as well as at the endpoint.



Source: Cascadia Labs[4]

Figure 2: Sophos Genotype Technology – top in independent tests

Simplifying HIPS with Genotype Technology

A Host Intrusion Prevention System (HIPS) aims to stop malware before a specific detection update is released, by monitoring the behavior of code.

Many traditional HIPS solutions monitor code only when it runs and then intervene if the code is deemed to be suspicious or malicious. The Sophos threat detection engine is different in that it analyzes the behavior of code *before* it executes and prevents it from running if it is considered to be suspicious or malicious. It combines this pre-execution analysis with runtime analysis to intercept threats, and SophosLabs rapidly validates the rule sets against terabytes of legitimate code, eliminating false positives.

Pre-execution analysis

Behavioral Genotype® Protection is foremost amongst Sophos Genotype technologies and protects the web, email and endpoint. Incorporated into the Sophos malware detection engine, it compares the genes from known families of malware with those of known bad content and behavior. By analyzing code before it executes and runs, Behavioral Genotype Protection can determine its functionality and the behavior it is likely to exhibit. This means that Sophos is able to detect malware earlier in the cycle than other vendors and eliminates the risk of partial infection or damage, which can be caused by relying purely on runtime analysis techniques.

> *Using Behavioral Genotype Protection, Sophos was able to proactively protect against 5,000 unique variants of Storm with just one identity.*

There are several hundred behavioral characteristics common across malware. Examples of these characteristics are:

- Using a packer (a compression tool that reduces the size of the executable)*
- Searching for publisher information
- Using a particular programming language
- Attempting to access the internet
- Containing certain strings
- Adding registry entries.

Gene identification

A gene can be recognized by the specific behavior it exhibits.

Example
If an application is packed, written in Visual Basic, accesses the internet and contains references to banking websites there is a very strong likelihood of it being a banking Trojan.

Behavioral Genotype Protection is complemented by suspicious file detection which alerts on files that exhibit suspicious behavior.

*21 percent of all malware in SophosLabs' collection is packed, compared to only 1 in 100,000 clean files.

Runtime detection

At runtime the endpoint is protected by:

- **Suspicious behavior detection** – watches all system processes for any signs of active malware, such as suspicious additions to the registry or file copying.
- **Buffer overflow detection –** looks for anything trying to use buffer overflow techniques to target security vulnerabilities, and protects both operating system software and applications.

SophosLabs experts do the fine tuning behind the scenes, automatically updating protection without the need for administrators to become experts in the latest malware techniques or system vulnerabilities.

Supporting malware detection technologies

Genotype and HIPS technologies are backed up by other techniques, including:

- Dynamic Code Analysis™ – a 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).

> *"Sophos scored 99.4% in an independent anti-spam test, beating IronPort and Clearswift[5]"*

Protecting against spam

To create lists of thousands of email addresses which they then distribute via botnets (networks of hijacked zombie computers), spammers use a variety of techniques including address harvesting from websites, newsgroup postings, and automatically generated "guessing" of addresses.

Spam campaigns cover a huge array of topics. Drug and loan campaigns have been joined by "pump and dump" campaigns, in which stocks are talked up to persuade people to invest in them, and then sold by the spammers at the artificially inflated price. These campaigns often exist for only a couple of hours, or even minutes, before mutating, and new techniques are constantly introduced to increase the chances of successfully avoiding detection. One of the more recent trends, for example, has been the sending of PDFs, MP3s, and other attachments.

By sending spam through "fresh" open proxies, spammers try to prevent their messages being blocked by IP-based block lists. To bypass reputation filtering, they register hundreds of new domains for each spam campaign, making it harder for security vendors to react. By randomizing obfuscation patterns and images, rotating phrases and adding random unrelated words and phrases, spammers can ensure that every recipient gets a message that looks different from others in the same campaign. These techniques impact the efficiency of spam detection signatures and basic content analysis. Spam emails that contain no call to action in the message (for example stock market scams) make call-to-action and URI analysis ineffective detection methods.

Leading-edge spam detection technologies

SophosLabs uses a combination of techniques to successfully detect and block spam (see figure 3), including the following range of leading-edge technologies:

- SXL (Sophos eXtensible List) – provides instant online access to the latest anti-spam intelligence from SophosLabs
- Traffix – uses global email traffic data collected by SophosLabs to identify spam sending hosts and networks
- Image attachment and fingerprinting – provides checksums against PDFs, JPGs, ZIPs, etc
- Destination URI extraction and other call-to-action identification – looks for known spammers' phone numbers and instant messaging IDs, as well as spammer websites and domains
- Identification of suspicious senders.

> *Sophos SXL provides instant online access to the latest anti-spam intelligence from SophosLabs.*

In addition to technologies like SXL and Traffix, Sophos uses a range of industry-standard approaches to identify and block spam including:

- Sender reputation filtering that cross-references the sender's IP address against the Sophos IP Block List, a list of known spammer IP addresses
- Heuristics filtering
- Scanning email subject and body content
- Obfuscation detection that catches content which has been disguised with, for example, letters substituted for numbers, e.g. V1agra.
- Automated tuning of all these techniques in response to evolving spammer tactics.

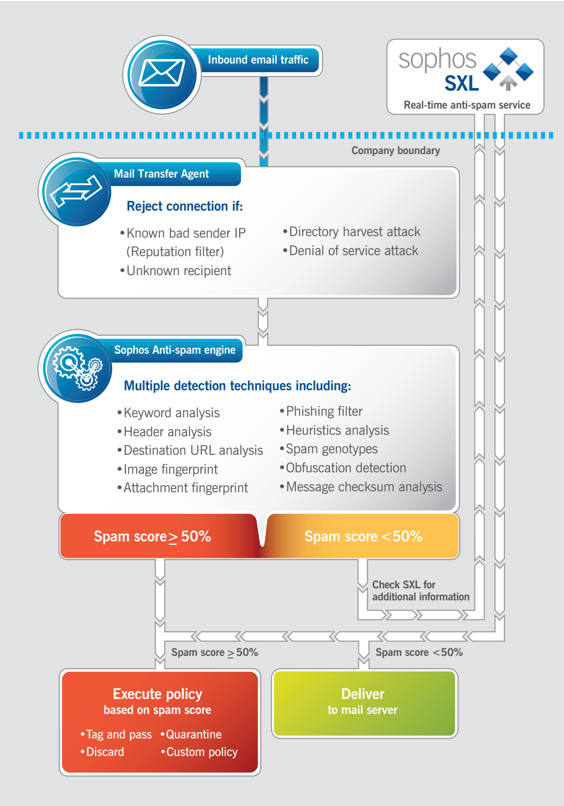


Figure 3: A multi-technique system for blocking modern spam campaigns

Proactive protection against spam campaigns

Genotype Technology, which provides such powerful protection against malware, also provides proactive detection against the latest mutations of a particular spam campaign. In blocking the spam it thereby also blocks the related malicious websites.

For each campaign, a unique genetic template is created which is then applied against incoming message traffic.

Examples of common genes that might be found in a particular spam campaign are:

- The presence of certain email headers and their attributes
- The URL found in the message ends with a .aspx string and is followed by a question mark and 5 to 7 digits
- The HTML part contains a table with three rows on a pink background.

Extra protection through alerts

Two alert services, ZombieAlert and PhishAlert, provide organizations with an extra level of service by informing them if any of their computers have been compromised and turned into zombies, or if their brand is being used in phishing campaigns.

Conclusion

SophosLabs is the industry's only research group with a truly integrated understanding of today's rapidly evolving threats. Its approach to combating spam, viruses and other malware involves a unique combination of expert analysis, automated systems and Genotype Technology. The integration of these core elements provides complete visibility of the threat landscape, resulting in the best, independently proven, proactive detection rates, with threats stopped before they launch whether they come from the web, email or endpoint devices. This round-the-clock, enterprise-wide protection has led to unrivalled customer satisfaction, with IT administrators given greater confidence in the security of their network and more time to concentrate on other business-critical issues.

Sophos products

SophosLabs' expertise underpins all Sophos's web, email and endpoint security and control solutions. To find out about any Sophos product, please visit www.sophos.com/products.

Sources

1 Security Threat Report 2008, www.sophos.com/pressoffice/news/articles/2008/01/security-report.html

2 www.sophos.com/pressoffice/news/articles/2008/01/storm-timezone.html

3 www.av-test.org, cited in blogs.pcmag.com/securitywatch/Results-2008q1.htm

4 www.cascadialabs.com/reports/Sophos_Endpoint_Security_for_Enterprises.pdf

5 Email appliances for the small/medium-sized business market, 16 Dec 2007, www.sophos.com/evision

About Sophos

Sophos enables enterprises worldwide to secure and control their IT infrastructure. Our network access control, endpoint, web and email solutions simplify security to provide integrated defenses against malware, spyware, intrusions, unwanted applications, spam, policy abuse, data leakage and compliance drift. With over 20 years of experience, we protect over 100 million users in nearly 150 countries with our reliably engineered security solutions and services. Recognized for our high level of customer satisfaction, we have an enviable history of industry awards, reviews and certifications. Sophos is headquartered in Boston, MA and Oxford, UK.

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

SOPHOS
WWW.SOPHOS.COM