

# Are you a spammer? Why stopping zombies dead in their tracks is essential

A Sophos positioning paper

November 2005

Hijacked computers, or zombies, hide inside networks where they send spam, steal company secrets, and are used in other serious crimes. This paper explains how businesses are under constant attack from this fast-moving threat, and how zombies can be created even in networks with reliable gateway and endpoint protection. The paper also outlines the need for organizations to protect themselves with a tool for detecting zombies and describes how Sophos ZombieAlert™ Service provides customers with this vital extra layer of security.

---

## Businesses under attack

A zombie is a computer that has been silently infected with a virus, giving unauthorized or remote users the ability to control it. Once a computer has been turned into a zombie, hackers use it to commit a wide range of crimes by linking with a network of thousands of other infected computers. Networks of zombie computers are used by hackers to send spam, viruses, phishing emails and pornography from within unwitting organizations. Sophos estimates that over 60% of all spam originates from hijacked computers. Zombies have been found in organizations of all kinds, from financial planning companies to universities and nursing homes. They cause business disruption, network damage, information theft and harm to an organization's reputation.

- **Business disruption:** Administrators are often unaware that there is a zombie on their network until the organization is listed as a spammer on a domain name server block list (DNSBL). This can cause corporate email failure, thereby crippling regular business functions.
- **Network damage:** Zombies aggressively attempt to infect other computers in an organization, slowing down internal networks. They are also used to store pirated software and films and hack into other organizations, consuming yet more network resources.
- **Information theft:** Confidential information such as client databases and bank account passwords are at risk of being stolen by zombies. Even encryption cannot protect information, since a zombie can install spyware (such as a keylogger) to capture every stroke made on a keyboard before sending the information to hackers.
- **Damage to reputation:** The illegal actions of zombies damage the reputation, image and brand value of a business if it is seen as sending spam or facilitating other crimes. For example, zombie networks are often

used to launch distributed denial of service (DDOS) attacks, where thousands of computers all access a website at once, overloading its servers and causing it to shut down.

## Fast and invisible

Zombies typically operate without end users' knowledge, and the damage they cause to organizations builds up unnoticed. For example, zombies are often programmed to keep their true nature hidden by "waking up" for very short periods in order to send spam before becoming dormant again.

---

*If an unprotected PC is connected to the internet, there is a 50% chance of it becoming a zombie within 12 minutes.*

---

As well as functioning silently, zombies are created extremely rapidly – Sophos research shows that if an unpatched PC without anti-virus protection or a firewall is connected to the internet, there is a 50% chance of it becoming a zombie within 12 minutes. The speed of these attacks is illustrated in figure 1. The graph shows how the probability of virus infection increases with time on an unprotected computer that is running Windows XP and is connected to the internet.

## A growing threat

The speed with which zombie networks can be created and their invisibility make them a very effective business tool for criminals. Zombies can generate significant income by installing adware or by stealing confidential information through spyware and phishing. Zombies can also install rogue dialers which run up large phone bills for affected users, or can be used to extort money from organizations with the

---

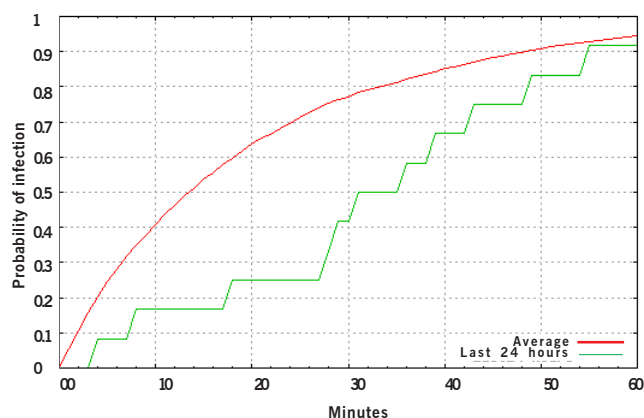


Figure 1: Probability of infection of an unprotected computer connected to the internet

threat of DDOS attacks. Zombie networks can even be sold themselves, with one report of a network of 20,000 PCs offered for sale on a spammer's forum for \$2,000 to \$3,000.<sup>1</sup>

The most common method of generating income through zombies, however, is to send spam. Anti-spam measures are becoming more effective at blocking spam emails based on the reputation of the sender, through the use of DNSBLs. Zombie networks counter the use of block lists by sending spam from hijacked computers with "clean" sender reputations. To facilitate the sending of spam, a continual supply of new zombies needs to be created in order to replace those which are identified and disinfected, and those which have been block listed.

As anti-spam techniques continue to improve, spammers will continue to recruit more zombies. The recent rapid growth in the number of zombie viruses illustrates this – of the most recent 300 viruses caught by SophosLabs™, a global network of threat analysis centers, over a third contained zombie functionality.

## How computers become zombies

A computer becomes a zombie when a bot, or automated program, is installed on it, giving a hacker control and making the computer part of a zombie network, or botnet. For the bot to be installed, an internet port needs to be opened in the computer. Back doors (open internet ports) are opened by viruses, worms or Trojan horses when they infect computers. After the back door is opened, the bot is installed, often by the same virus, and the computer becomes a zombie. In some cases it is hackers who install the bot, having searched for open ports through which they can access the computer.

One of the most common ways in which viruses infect computers and turn them into zombies is by exploiting operating system vulnerabilities. Viruses also spread through

social engineering techniques, where recipients of emails with a viral payload are tricked into activating them by opening an attachment or by clicking on a link. A common method of activating zombies once they have been created is to program them to monitor a chatroom. When the hackers type a specific command into the chatroom, the zombies "awake" and carry out their instructions. Zombies can also carry out pre-programmed instructions. For example, in May 2005, the Sober-Q Trojan horse and Sober-N worm worked in tandem to infect and hijack computers around the world, programming them to send out German nationalistic spam during an election.<sup>2</sup>

## Defending against zombie attack

The most effective protection against hackers gaining control over computers on a network is to complement endpoint and gateway solutions with a rapid and reliable zombie detection system. However, integrated protection of the desktop, workgroup, gateway and remote systems remains the baseline requirement.

### Gateway defense

The email gateway is the first line of defense for networks against email-borne viruses, including those which create zombies. Sophos PureMessage® provides a reliable, integrated solution for protection at the gateway using Genotype™ technology, a unique approach which automatically detects variants of both virus families and spam campaigns.

---

*Securing the email gateway is not enough – viruses can bypass the gateway to attack networks through a variety of other routes.*

---

However, securing the email gateway is not enough – viruses can bypass the gateway to attack a network through a variety of other routes:

- The internet – some worms that contain zombie functionality, such as Sasser and Rbot, do not spread via email. Instead they exploit vulnerabilities in operating systems or browsers to spread directly to desktops via the internet.
- Mobile devices – viruses can be introduced to desktops, and therefore the entire network, via devices such as USB flash drives, CDs and laptops that have been taken out of the organization and returned by employees.



However, the complexity of some networks, combined with the speed and intensity of attacks demands a contingency solution. Sophos ZombieAlert Service rapidly notifies organizations if any computers on their networks have become zombies, enabling enterprises to back up their protection with a reliable and fast solution in the event of zombie infection.

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

## Sources

- 1 How zombie networks fuel cybercrime, Celeste Biever, New Scientist, November 2004, [www.newscientist.com/article.ns?id=dn6616](http://www.newscientist.com/article.ns?id=dn6616)
- 2 Spamming Sober-Q Trojan horse stopped proactively by Sophos Genotype technology, Sophos, 16 May 2005, [www.sophos.com/virusinfo/articles/soberq.html](http://www.sophos.com/virusinfo/articles/soberq.html)

## 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 2005. 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 by any form or by any means without the prior written permission of the publishers.*

**SOPHOS**  
WWW.SOPHOS.COM