

Stopping zombies, botnets and other email- and web-borne threats

Hijacked computers, or zombies, hide inside networks where they send spam, steal company secrets, and enable other serious crimes. This paper discusses how the threat has evolved, explains how zombie networks, or botnets, are created and highlights how even organizations with reliable gateway and endpoint protection are vulnerable to these email- and web-borne threats.

Stopping zombies, botnets and other email- and web-borne threats

Businesses under attack

A zombie is a computer that has been silently infected with malware, 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, plant spyware and adware, and phish for confidential information from within unwitting organizations. Sophos estimates that up to 90% 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.

How computers become zombies

A computer becomes a zombie when a bot, or automated "software robot", is installed on it, giving a hacker control and making the computer part of a zombie network, or botnet. Once a zombie has been created it can then be used to turn other computers into zombies. For the bot to be installed, an internet port needs to be opened in the computer. Backdoors (open internet ports) are opened by viruses, worms or Trojan horses when they infect computers. After the backdoor is opened, the bot is installed, often by the same virus, and the computer becomes a zombie.

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.

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.¹

As well as functioning silently, zombies are created extremely rapidly, although the speed with which a computer is likely to become infected has reduced as more people are using Windows XP with SP2, which prevents them becoming infected through internet worms. Windows Vista is likely to reduce the vulnerability further. In response, zombie creators are turning to other methods to infect.

Bots can be replaced easily by malware writers as existing code is detected and blocked by security organizations.

Spam, botnets and websites are all used, as is the exploitation of operating system vulnerabilities. Toolkits can even be downloaded from the internet for free allowing zombies to be created quickly to exploit new operating system vulnerabilities before they are patched. By constantly developing new methods, cybercriminals have ensured that zombie

networks remain a very effective business tool – and the threat is growing. According to the SANS Institute, on any given day 3–3.5 million zombies are active around the world.²

A steady income stream

Zombies can generate significant income by installing adware or by stealing confidential information through spyware and phishing. They are also responsible for click fraud, which subverts the intention of pay-per-click online advertising by imitating a legitimately used web browser to click on an ad and accrue money for the zombie creator rather than the owner of the ad. 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 threat of distributed denial-of-service (DDoS) attacks.

Zombie networks can even be sold themselves, with one report of a network of 20,000 PCs offered for sale on a spammers' forum for \$2,000 to \$3,000.³ And in May 2006, Jeanson James Ancheta, a 21-year old hacker from Los Angeles, was given a 57-month jail sentence for running a network of 400,000 zombies.⁴ Ancheta admitted advertising his botnets online via an IRC channel entitled #botz4sale, and selling access to software that could remotely control computers to deliver spam and launch DDoS attacks against websites. He made more money by installing adware on the zombie computers, using the proceeds to pay for computer servers to carry out additional attacks.

As detection 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.

Defending against zombie attack

Integrated protection of the email and web gateways, desktops, workgroups, and remote systems remains the baseline requirement in defending networks.

The need for gateway protection

The gateway is the first line of defense against email- and web-borne viruses, including those which create zombies.

The most common method for a criminal to generate income through zombies 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

“Securing the web and email gateway is as critical as protecting the endpoint to ensure your network is not hiding zombies.”

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.

However, in a twist on earlier exploits, cybercriminals are turning to the web to take advantage of a generally low level of threat awareness among surfers, and the lower priority that web security often has within organizations. They send out spam that contains no malware itself, but directs the email recipient to malicious websites from which malware – including zombie-creating programs – is downloaded.

The need for endpoint protection

Zombie creators also use routes that bypass the web and email gateways so gateway protection needs to be complemented by equally robust endpoint protection against threats such as the following:

- 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.
- Instant messaging – IM applications bypass the email gateway, providing viruses with another entry route.
- Illegitimate SMTP servers – some viruses spread to other networks using their own SMTP server, enabling them to bypass the email gateway. The Trojan Spammit-F, which appeared in August 2006, is an example, as is the much older Bofra. In addition, once a zombie is created on a network, it may also use its own SMTP server to send spam directly from the infected machine, thus avoiding detection by outbound mail filtering systems.

Particularly in complex environments, where employees might be accessing the network remotely, central control over every computer to ensure up-to-date protection, is important as a single inadequately protected or infrequently updated computer risks infecting the network with zombies.

Organizational policies

It is also crucial to back up good endpoint and gateway protection with sound organizational policies. The continual onslaught on systems means zombies can result from the smallest and most temporary gap in security. Even with all points protected, any slips in policy – such as not keeping all operating systems on all computers fully patched – can allow computers to be hijacked.

Organizational policies such as educating end users in best security practice and disallowing access to file sharing and potentially infected websites have an important part to play. Use of a client firewall to block inbound and outbound internet ports which are not essential for communication also helps, by preventing hackers from gaining access to computers. In addition, by using an alert system that can detect zombies on its network, an organization will be able to shut down any infected computers as fast as possible.

Summary

Growing numbers of corporate computers are being hijacked, as zombie networks become more attractive to criminals. Zombies are hard to detect, and cause significant damage to businesses. Attacks on computers are fast and continuous, come from a variety of sources, and can occur through every entry point on the network. The complexity of some networks, combined with the speed and intensity of attacks demands enterprise-wide protection – effective defense against zombies must be an integrated gateway and endpoint solution ♦

The Sophos solution

Sophos PureMessage® and Sophos Email Security Appliances provide reliable, integrated software and hardware solutions respectively for protection at the gateway. Sophos Web Security Appliances prevent zombie-creating malware from being downloaded from malicious websites and also, uniquely, block any communication back out to the URL. The endpoints are protected from known and unknown threats by Sophos Anti-Virus®. All these solutions use Genotype® technology, a unique approach which automatically detects variants of both virus families and spam campaigns. Sophos Anti-Virus also includes Behavioral Genotype Protection which delivers the benefits of a Host Intrusion Prevention System (HIPS) by analyzing behavior before the code executes.

In addition, Sophos ZombieAlert is a unique service that notifies an organization within minutes of SophosLabs receiving a spam email from it. This enables the organization to back up its protection with a reliable and fast solution in the event of zombie infection. ZombieAlert information includes IP source information, message samples and information on any IP addresses on a customer network that are listed in third-party DNSBLs.

To find out more about Sophos products and how to evaluate them, please visit www.sophos.com

Sources

- 1 Spamming Sober-Q Trojan horse stopped proactively by Sophos Genotype technology, Sophos, 16 May 2005, www.sophos.com/virusinfo/articles/soberq.html
- 2 When bots attack, 6 April 2006, www.baselinemag.com
- 3 Going price for network of zombie PCs: \$2,000 - \$3,000, Byron Acohido and Jon Swartz, USA Today, www.usatoday.com/tech/news/computersecurity/2004-09-08-zombieprice_x.htm
- 4 57 months in prison for 21-year-old hacker who ran zombie network, Sophos, 9 May 2006, www.sophos.com/pressoffice/news/articles/2006/05/anchetasentence.html

About Sophos

Sophos is a world leader in integrated threat management solutions purpose-built for business, education and government. With 20 years' experience and consolidated anti-virus, anti-spyware and anti-spam expertise SophosLabs protects even the most complex networks from known and unknown threats. Our reliably engineered, easy-to-operate products protect over 35 million users in more than 150 countries from viruses, spyware, intrusions, unwanted applications, phishing, spam and email policy abuse. Round-the-clock vigilance has resulted in our increasingly rapid international growth, expanding user base and continuous profitability. Our instant response to new threats is matched by business-focused, 24/7 technical support, and has led to 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 by any form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM