

# Managing Security Risks in Modern IT Networks



White Paper



## Table of Contents

Executive summary .....	3
Introduction: networks under siege .....	3
How great is the problem? .....	3
Spyware: a growing issue .....	3
Feeling vulnerable .....	4
An evolving security response .....	4
Towards a managed environment .....	4
The wider picture .....	5
Conclusion and recommendations .....	5

This document contains confidential and proprietary information of LANDesk Software ("LANDesk") and its affiliates and is provided in connection with the identified LANDesk product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk's terms and conditions of sale for such products, LANDesk assumes no liability whatsoever, and LANDesk disclaims any express or implied warranty, relating to sale and/or use of LANDesk products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct, or modify this material, including any specifications and product descriptions, at any time, without notice.

Copyright © 2004, LANDesk Software Ltd., or its affiliated companies. All rights reserved.

LANDesk, Targeted Multicast and Peer Download are either registered trademarks or trademarks of LANDesk Software, Ltd. or its controlled subsidiaries in the United States and/or other countries.

\*Other brands and names are the property of their respective owners.

LSI-0363

## Executive summary

As businesses grow to rely more and more on network technologies for their profitability, so they are increasingly subjected to a growing range of network-based threats, from computer viruses to 'malware', malicious programs that can be exploited by hackers. The growing risk that this presents is driving a re-evaluation of the way in which networks are secured. In particular, it is becoming evident that security fixes and patches need to be applied network-wide the instant they become available, if they are to be effective against an increasing level of so-called 'day-zero' threats.

This paper examines the costs and benefits of managing security updates and concludes that, despite an obvious up-front expense, the purchase of an automated patch management system that includes a spyware threat analysis feature (such as can be found in the newly-launched Security Suite from LANDesk®) can prove a valuable investment in freeing up IT personnel time and protecting your company's network assets.

## Introduction: networks under siege

Never have computer networks been so valuable in business – and so difficult to keep safe. High-profile virus outbreaks such as MyDoom or Blaster serve to keep IT security in the headlines, but the unfortunate reality is that network threats are now so commonplace that they have all but ceased to be newsworthy.

## How great is the problem?

As a backdrop to more detailed risk assessment, it is worth restating some salient statistics on network security:

- In Europe, 61 per cent of businesses see spyware as a major security issue and half consider themselves 'challenged' when removing it from the network; 44 per cent are searching their network every week for threats<sup>1</sup>.
- In a Gartner survey of chief information officers' top business trends for 2004, the combined rankings of security breaches and data protection indicate that security is the highest-rated business trend this year.
- Carnegie Mellon University's CERT Coordination Center logged 3,784 security vulnerabilities in 2003.
- The Center also stated that most intrusions result from exploitation of known vulnerabilities, configuration errors or attacks where countermeasures were available.
- In the US<sup>2</sup>, 85 per cent of organisations were hit by viruses in 2002, even though 98 per cent had firewalls and 99 per cent had anti-virus programs.
- Malicious code caused damage worth US\$13 billion worldwide in 2001.
- In 1999, Fortune 1,000 firms lost US\$45 billion from theft of information and were hit by an average of 67 attacks.
- Business and government entities worldwide spend in excess of US\$2 billion annually to investigate, assess and deploy security patches.<sup>3</sup>

Going forward, networks are likely to become even less secure.

In order to boost worker productivity, businesses are keen to promote web-based mobile working practices and there is growing corporate use of new applications such as Instant Messaging (IM), media players or, potentially, peer-to-peer (P2P) networking programs.

According to Forrester Research from 2003, there will be 35 million remote users by 2005 and 14 billion devices on the Internet by 2010.

However, these trends compromise network security and are being widely exploited by hackers and malicious code writers - 19 of the top 50 viruses and worms in the spring and summer of 2003 propagated using P2P and IM, a 400 percent increase over the level of the previous year<sup>4</sup>.

## Spyware: a growing issue

Many P2P applications promote the spread of 'spyware' or 'adware', intrusive code that logs activity by the user and reports it back to a remote server. A study by the University of Washington, for example, found the popular file-sharing program Kazaa came bundled with no less than 12 different spyware or adware applications.

<sup>1</sup>Omniboss survey for LANDesk, November 2004.

<sup>2</sup>Computer SI/FBI Computer Crime and Security Survey, 2002

<sup>3</sup>The Aberdeen Group

<sup>4</sup>Symantec Internet Security Threat Report, October 2003

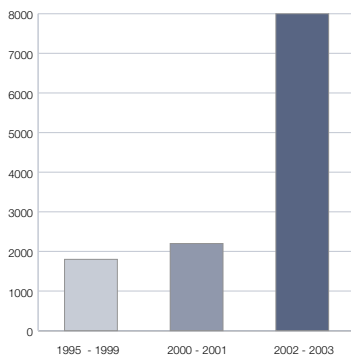
This is a growing problem for IT managers. Nine out of 10 PCs connected to the internet are said to be infected with spyware<sup>5</sup> and there are an average of 27.5 spyware traces on any given machine<sup>6</sup>; 92 per cent of IT managers at companies with more than 100 employees claim they have a 'major' spyware problem<sup>7</sup>.

Software vendors have only just begun to respond to this problem, with the LANDesk Security Manager being one of the first products on the market to specifically offer support in combating the spyware threat.

## Feeling vulnerable

What systems are susceptible to attack? The simple answer is any, and all. A review of the vulnerabilities logged by the Cassandra tracking tool<sup>8</sup> shows Microsoft's products are the most affected by vulnerabilities but Linux has, since January 2000, had more than any single Microsoft system. IT purchasers may find themselves with a dilemma when specifying systems: those that are most popular tend to be the ones that are most frequently updated, and therefore likely to pick up vulnerabilities.

Diagram 1: vulnerabilities are rising



Source: Gartner, August 2004

## An evolving security response

Over time, the increasing prevalence of networks and network-based threats has led to an evolution of the security response. Early on in the development of the Internet, the response to security threats was often not until both a potential weakness had been uncovered and an actual attack had been experienced.

This quickly moved to a position where network administrators tried to prevent attacks using anti-virus programs to combat known threats. Now the situation has progressed further, towards a 'stop counting attacks, start closing gaps' philosophy, with efforts focusing on plugging weaknesses, through software patches, before they have even necessarily been exploited maliciously. This clearly improves the security of the network, but creates an onerous burden for network managers.

Each patch has to be brought in house, tested and installed on every computer. Gartner<sup>9</sup> estimates that the task of patching Windows 2000 and XP operating systems alone can increase desktop total cost of ownership by around US\$200 per user, per year, while adding up to 20 per cent to labour costs. This does not take account of the opportunity loss arising from dedicating limited, skilled IT personnel resources to relatively mundane patch management tasks.

## Towards a managed environment

Given the above, it is hardly surprising that moves are afoot to automate security functions so that they remain active and up to date without operator intervention.

At the network level, vendors such as Cisco Systems now offer integrated security in devices such as routers and switches. With regards to PC maintenance, meanwhile, it is now possible to purchase patch management systems that allow network managers to retain complete control of their networks, while greatly simplifying and speeding up the process of applying security patches across hundreds or even thousands of machines.

<sup>5</sup>National Cyber Security Alliance, June 2003

<sup>6</sup>Earthlink/Webroot spy audit report

<sup>7</sup>Web@Work study, March 2004

<sup>8</sup><https://cassandra.cerias.purdue.edu/main/>

<sup>9</sup>Security Holes Increase Windows Client TCO, October 2004

Typically, an industry-leading patch management system will provide a number of discrete services, such as:

- Identifying the current state of a company's IT systems.
- Assessing known vulnerabilities.
- Reviewing the status of vulnerabilities detected.
- Deploying required patches.
- Setting policies to ensure updates are applied based on corporate standards.

Do these systems offer value for money? An IDC study<sup>10</sup> compared companies using LANDesk Management Suite 8 patch management systems against those using traditional 'point product' methods and found that the former saved an average of almost US\$1.1 million (equivalent to US\$22,909 per 100 users) annually over three years in increased productivity, as a result of reduced downtime. The system paid for itself in just over 90 days.

## The wider picture

Simple economic comparisons such as this do not, however, provide a complete view of the benefits of a managed system. The reduction in downtime quoted by IDC reflects an improved ability of the network (and therefore the business) to defend itself. At a time when day-zero attacks can potentially cripple key systems, this added security not only represents a productivity gain but is clearly an important form of insurance. For companies that have a large IT department and can afford to spare the resource, managing security patches in the traditional way may still be viable for some time. However, there is increasing evidence that, for the average business, it makes sense to buy in the resources and outsource the risk by committing to a specialist patch management system.

This thinking is reflected in predictions for the growth of the patch management software market, which was estimated to be worth US\$ 17.8 million in 2003 and is tipped to mushroom to more than US\$42 million by 2007.

## Conclusion and recommendations

Patch management systems have been on the market long enough now for their efficacy to be proven. They are widely-enough employed to ensure they will not cause interoperability or integration problems. And the case for using them is growing by the day.

As a result, LANDesk recommends that patch management systems should be evaluated as part of the overall IT security response as soon as is practicable. This evaluation should incorporate two separate analyses:

1. A financial/manpower analysis to gauge current and predicted expenditure on manual patch management versus an automated system.
2. A risk analysis to gauge the potential losses to the business in the event that IT security is compromised through some of the weaknesses inherent in a manual patch management process, such as delays in applying patches, the potential for patches to be applied incorrectly and so on.

In the event that an automated patch management system is considered necessary – and it is expected that this will be in the majority of cases – then it is important to purchase a system that offers the widest possible range of features and covers the full array of operating systems and applications that might be incorporated into the corporate network. Key features to look for include:

- Centralised research and investigation of designated systems software to ensure rapid detection of new vulnerabilities.
- Threat assessment that compares each computer's configuration to a vulnerability database.
- Patch validation and automated downloading to increase the reliability of the system and avoid having to re-patch.
- Spyware threat analysis support.

Patch management is of course just one aspect of IT security and should be viewed in the context of a wider strategy that potentially encompasses everything from disaster recovery planning to staff training. However, given the prevalence of network-borne threats that exploit vulnerabilities in applications and operating systems, it is worth making a review of patch management a major priority.

<sup>10</sup>Quantifying the ROI Benefits of Integrated Systems Management, October 2004