Chapter 6.12
Malware and Antivirus Deployment for Enterprise Security

Raj Sharman
State University of New York at Buffalo, USA

K. Pramod Krishna
State University of New York at Buffalo, USA

H. Raghov Rao
State University of New York at Buffalo, USA

Shambhu Upadhyaya
State University of New York at Buffalo, USA

ABSTRACT

Threats to information security are pervasive, originating from both outside and within an organization. The history of computer security is dotted with the tales of newer methods of identification, detection, and prevention of malware, only to be followed by a new set of threats that circumvent those safeguards. The explosive growth of the Internet and wide availability of toolsets and documentation exacerbates this problem by making malware development easy. As blended threats continue to combine multiple types of attacks into single and more dangerous payloads, newer threats are emerging. Phishing, pharming, spamming, spoofing, spyware, and hacking incidents are increasing at an alarming rate despite the release of breakthrough security defense products. A multi-layered, integrated approach using different security products in conjunction with well-defined security policies and antivirus software will form the foundation for effective enterprise security management.

INTRODUCTION

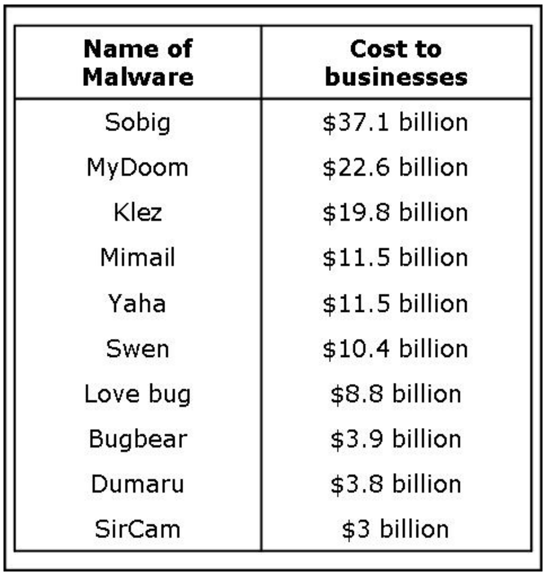
Enterprise deployment refers to uniform distribution, operation, administration, and maintenance of a common solution across all departments in a given organization. The strategies and teachings from this chapter apply to all organizations, large and small, as long as an enterprise deployment solution is used. The increased use of the information superhighway has been accompanied, inevitably, by a commensurate increase in the incidence and impact of malware outbreak. A malware attack is more pernicious than other forms of *information security* (IS) vulnerabilities in that its impact is generally not confined to one or a few entities; rather, it is normal for a large number of organizations to be affected at once, to a substantial degree. The scale of impact determines the scale of damage. Deployment strategies are therefore crucial, not only to prevent attack, but to also contain the spread of impact once vulnerability at some point has been maliciously exploited. Antivirus software has evolved over the last decade to become, along with firewalls, one of the main defenses against malware invasion and a primary tool in the maintenance of information security. To be sustainable, security must be aligned with business practices and priorities, as well as with the overall corporate IS policy. This chapter begins with a brief introduction and discussion on the history of viruses and of the emergence of antivirus software. Later sections present an approach to protection against malware, integrating antivirus software, firewalls, IDS, and other security applications into a practicable framework. Finally, the chapter concludes with a detailed discussion on the mechanics of malware and of antivirus software.

MALWARE AND ITS IMPACT

Malware is short for malicious software and is typically used as a catch-all term to refer to the class of software designed to cause damage to any device, be it an end-user computer, a server, or a computer network. Among the many forms malware can assume are that of a virus, a worm, a Trojan, spyware, or "backdoor," among others.

Malware on the Internet is not only massive in sheer quantity but also prorate. In August of 2003, McAfee, an anti-malware software manufacturer, identified fewer than two million malware products on the Internet; less than a year later, in March of 2004,; as many as 14 million such products were detected by the same company (Argaez, 2004). This rate of increase is expected to continue in the foreseeable future. The damage caused by all this malicious software is humungous. Table 1 enumerates ten malware programs and the estimate of the damage caused by them to businesses worldwide.

Table 1. Cost to businesses due to Malware outbreak [Source:(Mi2g, 2004)]



Name of Malware	Cost to businesses
Sobig	$37.1 billion
MyDoom	$22.6 billion
Klez	$19.8 billion
Mimail	$11.5 billion
Yaha	$11.5 billion
Swen	$10.4 billion
Love bug	$8.8 billion
Bugbear	$3.9 billion
Dumaru	$3.8 billion
SirCam	$3 billion

Related Content

Hybrid Optimization and Deep Learning for Detecting Fraud Transactions in the Bank

Chandra Sekhar Kolliand Uma Devi T. (2022). *International Journal of Information Security and Privacy (pp. 1-20).*

www.irma-international.org/article/hybrid-optimization-and-deep-learning-for-detecting-fraud-transactions-in-the-bank/300323

Homo Electricus and the Continued Speciation of Humans

Katina Michael (2007). *Encyclopedia of Information Ethics and Security (pp. 312-318).*

www.irma-international.org/chapter/homo-electricus-continued-speciation-humans/13490

Machine Learning Interpretability to Detect Fake Accounts in Instagram

Amine Sallah, El Arbi Abdellaoui Alaoui, Said Agoujiland Anand Nayyar (2022). *International Journal of Information Security and Privacy (pp. 1-25).*

www.irma-international.org/article/machine-learning-interpretability-to-detect-fake-accounts-in-instagram/303665

Introduction of Blockchain and Usage of Blockchain in Internet of Things

Chandrasekar Raviand Praveensankar Manimaran (2023). *Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 37-48).*

www.irma-international.org/chapter/introduction-of-blockchain-and-usage-of-blockchain-in-internet-of-things/310438

Threshold Secret Sharing Scheme for Compartmented Access Structures

P. Mohamed Fathimaland P. Arockia Jansi Rani (2016). *International Journal of Information Security and Privacy (pp. 1-9).*

www.irma-international.org/article/threshold-secret-sharing-scheme-for-compartmented-access-structures/160771