SECURITY TRENDS

Overview

IRONPORT™

The Rising Threat of Email-Borne Spyware

SECURITY TRENDS

OVERVIEW

The explosive growth of spyware is an alarming trend that threatens to undermine the stability of the internet. Spyware has had a significant impact on consumer productivity: Microsoft estimates that spyware causes more than half of all Windows system crashes and a 2004 Dell report shows that over 20 percent of support calls were spyware related, up from just 1% a year earlier. But the effects of spyware aren't just measured in lost productivity. Spyware is threatening the security and privacy of businesses and consumers. In August, for example, data stolen by spyware was discovered on a U.S.-based server. The server contained passwords for online accounts from 50 different banks, eBay and PayPal logins, hundreds of credit card numbers, and large amounts of personal data.

TRENDS & SOLUTIONS

Why has the spyware threat grown so quickly? In short, it is the money. Hackers use malicious spyware such as Trojan horses, keyloggers, and screen captures to steal and profit from valuable personal and financial information. Hackers also profit by hijacking infected PCs and using them to launch money-generating spamming, phishing, denial of service, and additional spyware attacks.

Increasingly, hackers are turning to email as a spyware distribution vector. Email has long been the primary medium for virus writers because it has the unique ability to quickly spread and lends itself to social engineering. Email is also advantageous to hackers because it can be written to morph to avoid AV signature detection. And email can be used to distribute malicious payloads either as an attachment or through a malicious URL, inserted into an email, which attacks victims when the link is accessed. Hackers have realized the power of email as a distribution vector and have begun using email to launch spyware attacks. In fact, in August of 2005, 60 percent of the top 10 email threats had some type of spyware functionality (Trojan back doors, key loggers), up 200% from a year ago.

> **"IronPort Virus Outbreak Filters is the ideal solution to combat the rising threat of email-borne spyware."**

Both reactive anti-virus signature solutions and preventive protection methods are needed to fully protect users from the email-borne spyware threat. A preventive solution should be able to quickly detect the spread of email-borne spyware. It also needs the ability to accurately block these attacks, whether they come from email attachments or blended threats such as malicious URLs contained in emails. Solutions that rely solely on heuristic-based or automated mass pattern detection technology are ineffective against quickly morphing and blended threats. In-depth, real-world traffic analysis—combining the best automated outbreak recognition techniques with human oversight—is the optimal way to detect attacks.

IronPort Virus Outbreak Filters™ is the ideal solution to combat the rising threat of email- borne spyware. Virus detection is based on *SenderBase*,® the world's largest traffic monitoring network. *SenderBase* has a view into a remarkable 25 percent of the world's email traffic.

IronPort's technology uses historical *SenderBase* data to create a statistical view of normal global traffic patterns. Real-time data from the global *SenderBase* network is processed by IronPort's virus detection technology and compared with the baseline, automatically identifying anomalies that are proven predictors of a virus outbreak. *IronPort Threat Operations Center* (TOC) analysts review the data on a 24x7 basis and issue rules based on numerous matrixes including file name, file keywords, file size, attachment type, file signature, and message URLs to quarantine suspicious traffic until anti-virus signatures are available. *IronPort Virus Outbreak Filters* complements traditional anti-virus solutions to detect and protect customers from emerging threats such as email-borne spyware.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

IronPort sales representatives, channel partners, and support engineers are ready to help you evaluate how IronPort products can make your email infrastructure secure, reliable, and easier to manage. If you believe that your organization could benefit from IronPort's industry leading products, please call 650-989-6530 or visit us on the web at www.ironport.com/leader

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, CA 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems.

SENDERBASE FAQ
10/05
DOC RELEASE