



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

Issue 32

Publication date: 31/01/07

Contents

- Technology Predictions 2007
- Non-OS-Dependant Malware
- One Hacker Kit Accounts For 71% Of December Web-Based Attacks
- Spear Phishing – Casting a Narrow Net
- Commonsense Guide to Prevention & Detection of Insider Threats
- Review of Secunia's "Software Inspector" - Detects Insecure Application Version
- Network Access Control Learning Guide
- Identity Theft
- Internet Threat Outlook Finds Rise in Sophisticated Attacks Against Savvy PC Users
- IEEE 802.11n Working Group Approves Draft 2.0

CCIP Contact Details:

T: +64 (0)4 498-7654
F: +64 (0)4 498-7655
E: info@ccip.govt.nz

<http://www.ccip.govt.nz/>

Technology Predictions 2007

Deloitte Touche Tohmatsu

This study examines ten emerging trends sure to have a major influence on the technology sector.

Source: <http://www.deloitte.com/>

Non-OS-Dependant Malware

IT-Observer

All too often people talk about the disadvantages of the Windows operating system: it has too many security flaws, it is not properly patched, it is not security oriented... Until the much talked about Vista system finally reaches our computers, there will still be plenty of time to protest.

However, with the new malware dynamic, the idea that malware is restricted to specific operating systems is becoming anachronistic. It no longer matters whether the victim is a home-user or a company employee. It is now irrelevant whether the system administrator is just someone who lives round the corner or a highly qualified IT manager.

Source: <http://www.it-observer.com/>

One Hacker Kit Accounts For 71% Of December Web-Based Attacks

InformationWeek

A multi-exploit hack pack was responsible for nearly three-fourths of all Web-based attacks during December.

Source: <http://www.informationweek.com/>

Spear Phishing – Casting a Narrow Net

nist.org

If you haven't heard of the term "Spear Phishing" you probably don't work for the Department of Defense (DoD). All DoD employees and contractors (Army, Navy, Air Force, Marines, etc.) are now required to complete spear phishing training. What is it and why should you care?

Source: <http://www.nist.org/>

Commonsense Guide to Prevention & Detection of Insider Threats

Carnegie Mellon University CyLab

In 2005, the first version of the Commonsense Guide to Prevention and Detection of Insider Threats was published by Carnegie Mellon University's CyLab. The document was based on the insider threat research performed by CERT, primarily the Insider Threat Study conducted jointly with the U.S. Secret Service (USSS). Over the past year, CERT has continued analyzing insider threat cases with the USSS. CERT has also conducted additional insider threat research funded by Carnegie Mellon CyLab and the U.S. Department of Defense Personnel Security Research Center. Those projects have involved a new type of analysis of the insider threat problem focused on high-level patterns and trends observed in the cases. Specifically, the projects examine the problem in terms of the interaction of insider psychology, organizational culture, policies, practices, and technology over time.

Source: <http://www.cert.org/>

Information Security Links

National Infrastructure Security Co-ordination Centre (NISCC)

Public Safety and Emergency Preparedness Canada (PSEPC)

United States Computer Emergency Readiness Team (US-CERT)

CERT Coordination Center (CERT/CC)

Australian Computer Emergency Response Team (AusCERT)

Internet Storm Center (ISC)

US-CERT Cyber Security Bulletins

Safe Computing Links

The Internet Safety Group (NZ)

CCIP Security Tips

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

Review of Secunia's "Software Inspector" - Detects Insecure Application Version

nist.org

Secunia has released a free on-line scanner that determines if your Windows 3rd party software has security updates available. The scanner works through your web browser and we found it surprisingly well thought out.

Source: <http://www.nist.org/>

Network Access Control Learning Guide

SearchSecurity.com

From PDAs to insecure wireless modems, users have myriad options for connecting to -- and infecting -- the network. Created in partnership with our sister site SearchWindowsSecurity.com, this guide offers tips and expert advice on network access control. Learn how unauthorized users gain network access, how to block and secure untrusted endpoints, and get Windows-specific and universal access control policies and procedures.

Source: <http://searchsecurity.techtarget.com/>

Identity Theft

McAfee Avert Labs

Businesses and governments ask us to reveal personal data more frequently than ever before. These institutions store this sensitive information in numerous, increasingly larger databases. This data is, of course, very valuable, but not only to those who should have it. Criminals also try to get their hands on this information, so that they can use it for malicious purposes or sell it to commit fraud. This is identity theft.

Source: <http://www.mcafee.com/>

Internet Threat Outlook Finds Rise in Sophisticated Attacks Against Savvy PC Users

Computer Associates

Computer Associates issued a report that warns of a new level of cyber-crime potential as increasingly sophisticated attackers aim to steal intellectual property, personal identities and the contents of bank accounts across international borders, and within organizations and social networks

Source: <http://www3.ca.com/>

IEEE 802.11n Working Group Approves Draft 2.0

Infoworld

After much debate and a lot of contention among the overall IEEE membership, the all-important IEEE 802.11n working group has given its stamp of approval to the next draft version of the specification.

Temporarily dubbed draft version 1.10, it will go out as version 2.0 when it is released to the full IEEE 802.11n committee, about 400 strong, by the end of the month.

Source: <http://www.infoworld.com/>



AGAINST CYBER THREATS

While this e-bulletin is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this e-bulletin.

CCIP only issues those external alerts that we assess as serious and would affect a large number of New Zealand users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this e-bulletin in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions expressed herein may not be used for advertising or product endorsement purposes.