



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

Issue 37

Publication date: 13/04/07

Contents

- Digital Strategy: The '3 C's' – are we making waves?
- Attack of the Bots
- Web 2.0 Users Open a Pandora's Box of Security Problems
- Old-Timers Top Malware Chart but Web-Based Threats Pose Greater Problems
- Schneier says Full Disclosure of Vulns a 'Damned Good Idea'
- The Current State of PHP Security (w/ MOPB full review)
- Fortify Software Documents Pervasive & Critical Vulnerability in Web 2.0
- Free AntiRootkit Software
- The Security Risks of Google Notebook

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/>

Digital Strategy: The '3 C's' – are we making waves?

Ministry of Economic Development

The government views information and communications technology (ICT) as a vital component to lifting New Zealand's economic performance and one of the foundations to achieve our economic, cultural, environmental and social goals.

For this reason, the government developed a Digital Strategy for New Zealand.

The Digital Strategy provides a clear view of the future we want create, and a plan for how to get there. The key enablers of the Strategy are Connection, Content and Confidence.

Broadband Connection should be fast, affordable, and available everywhere. Digital Content needs to be diverse, high quality, and of value to New Zealand users. Technology must be designed with people in mind who must have the capability and Confidence to use it well, to fully enrich their lives.

Source: <http://news.business.govt.nz/>

Attack of the Bots

Wired

The latest threat to the Net: autonomous software programs that combine forces to perpetrate mayhem, fraud, and espionage on a global scale. How one company fought the new Internet mafia – and lost.

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

Web 2.0 Users Open a Pandora's Box of Security Problems

Computerworld

Google Apps, ThinkFree Office and other hosted Microsoft Office alternatives are gaining in popularity as ad hoc collaboration tools. But such software-as-a-service (SaaS) offerings have few, if any, service-level or security guarantees and can leave a trail of potentially sensitive data on publicly accessible servers on the web.

Source: <http://computerworld.co.nz/>

Old-Timers Top Malware Chart but Web-Based Threats Pose Greater Problems

Sophos

The figures, compiled by Sophos's global network of monitoring stations, show that the Netsky family has had the biggest impact on computer users this month, accounting for almost a third of all malware seen during March.

Netsky's return to the top comes despite protection against this family of worms having been available for more than three years. Interestingly, just 0.18 percent or one in 555 emails was infected in March, yet Sophos detected 8,835 new threats, bringing the total protected against to 231,548. These numbers indicate that while malware spreading via email is still causing trouble, the vectors used to distribute threats are changing: hackers are continuing their move away from mass-mailing worms in favour of using spam messages with links pointing to infected webpages.

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

Information Security Links

Centre for the Protection of National Infrastructure (CPNI)

Canadian Cyber Incident Response Centre (CCIRC)

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)

Schneier says Full Disclosure of Vulns a 'Damned Good Idea'

Computerworld

Full disclosure -- the practice of making the details of security vulnerabilities public -- is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure. Unfortunately, secrecy sounds like a good idea. Keeping software vulnerabilities secret, the argument goes, keeps them out of the hands of the hackers. The problem, according to this position, is less the vulnerability itself and more the information about the vulnerability.

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

The Current State of PHP Security (w/ MOPB full review)

SPI Dynamics

The Month of PHP Bugs (MOPB) has concluded, and thus it's time to review the state of PHP security. Those of you who read my MOPB mid-month analysis are already familiar with the concept: take the pile of MOPB bugs, analyze their impact, and correlate it back to the development fix. Rather than just recap the second half of the MOPB initiative, I thought I would take this report a bit further and talk about some ways to reduce the attack surface of PHP, and comment on some PHP security observations I made while making these analyses.

Source: <http://portal.spidynamics.com/>

Fortify Software Documents Pervasive & Critical Vulnerability in Web 2.0

Fortify Software

Advisory details a fix for ubiquitous JavaScript Hijacking vulnerability that allows an attacker to emulate a Web 2.0 user's identity to fraudulently access software applications

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

Free AntiRootkit Software

Jose Nazario, Arbor Networks

As a complement to a recent post I made here with a list of free online AV scanners, I'd like to share with you a list of free AntiRootkit software for your PC. Especially in light of this past week's ANI-related malware spate and the new Grum Trojan, you should make sure that you're always on the lookout for threats. In the past few weeks we've seen even more malware that was simply not detected by AV.

Source: <http://asert.arbornetworks.com/>

The Security Risks of Google Notebook

SearchSecurity

In May 2006, Google released Google Notebook, a Web-based application with which users can save information they find on the Web, including snippets of Web pages, related notes, search results, images, and almost anything else. Google Notebook is similar to Web services like Yahoo's MyWeb, Ask.com's MyStuff, del.icio.us and digg.com, which provide a useful function to store and organize notes. But as Spider-Man's mantra reminds us, with great power comes great responsibility.

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