



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

Issue 38

Publication date: 27/04/07

Contents

- Sweetening the Honeygot
- Internet Security Threat Report
- Study Links Staff Use of Web 2.0 to Security Risks
- Image Spam: Getting the Picture?
- Polymorphic Viruses Call for New Antimalware Defenses
- Notes on Vista Forensics
- The Future of Security
- SCADApedia
- First Workshop on Hot Topics in Understanding Botnets (HotBots '07)
- Profile of a Fraudster Survey 2007

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/>

Sweetening the Honeygot

Dark Reading

New free tools and services aimed at making honeynets more manageable are now becoming available: The Honeygot Project next month will roll out its new Global Distributed Honeygot as well as new honeynet tools, Dark Reading has learned, while the New Zealand Honeygot Alliance has begun offering client-based honeynet services for organizations that can't run their own servers.

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

Internet Security Threat Report

Symantec

This volume of the Internet Security Threat Report offers an overview of threat activity between July 1 and December 31, 2006. The current Internet security threat environment is characterized by an increase in data theft, data leakage and the creation of malicious code targeting specific organization for information that can be used for financial gain. Attackers are now refining their methods and consolidating their assets to create global networks that support coordinated criminal activity.

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

Study Links Staff Use of Web 2.0 to Security Risks

Computerworld

UK firms are at risk of data leakage through their employees' increasing use of Web 2.0 technologies and social networking websites, security experts have warned.

A survey of more than 1,000 office workers found that 42% of those aged between 18 and 29 discussed work-related issues on social networking sites and blogs.

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

Image Spam: Getting the Picture?

IT-Observer

Spam. We've all seen enough of it. But just as familiarity has bred contempt (and stopped most email users responding to it), spammers have come up with a new technique to snare the unwary and get around corporate security measures.

The spammers' latest technique involves image spam – emails that contain little more than an image embedded into the body of the message. The image, of course, contains the spam message that you hoped to avoid.

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

Polymorphic Viruses Call for New Antimalware Defenses

SearchSecurity.com

Attackers are always looking for innovative ways to dodge antivirus software, and many malicious hackers are now creating polymorphic code to do just that. But it's not just malware writers who are raising the bar.

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

Notes on Vista Forensics

SecurityFocus

While the fundamental principles of computer forensics remain largely unchallenged, the landscape upon which investigators operate is constantly changing. A combination of new technologies and changing habits of use means that forensic examiners must always strive to keep up to date with the latest developments. One of the most anticipated new product releases this year is the Microsoft operating system Windows Vista. Vista was under development for a long time with Microsoft promising a raft of new features together with major improvements to security.

Source: Part 1: <http://www.securityfocus.com/infocus/1889> Part 2: <http://www.securityfocus.com/infocus/1890>

The Future of Security

McAfee

The second issue of McAfee Avert Labs security journal gazes into the crystal ball to divine what threats and defenses will attract your attention during the next five years.

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

SCADApedia

Digital Bond

Digital Bond's SCADApedia is a moderated wiki on control system and SCADA security. This is another in our continuing efforts to bring information on SCADA security to the control system community. The SCADApedia is a place for facts, while the SCADA Security blog is the place for opinions and news. For example, a SCADApedia entry on Rockwell Automation security would state the security features available in the products. The SCADA Security blog may give our opinion of the Rockwell Automation security and link to the SCADApedia entry for the facts.

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

First Workshop on Hot Topics in Understanding Botnets (HotBots '07)

usenix.org

HotBots (was) intended as a forum for lively discussion of innovative ideas, recent progress, or practical experience in understanding all aspects of botnets. HotBots '07 was co-located with the 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI '07), which took place April 11–13, 2007.

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

Profile of a Fraudster Survey 2007

KPMG

At first glance, an average fraudster¹ is not much different from an average person. Consequently, it is often extremely difficult to detect fraudulent acts. But upon reflection, the following circumstance must be considered: Why are people often caught unaware when somebody is accused of fraud? Because it is usually the colleague who is known to be helpful, polite and inconspicuous. But most importantly it is the colleague that enjoys the absolute trust of both superiors and colleagues.

Source: <http://www.kpmg.co.uk/>



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.