

## Issue 43

Publication date: 03/08/07

### Contents

- Security not a Benefit of Virtualisation
- Secunia Personal Software Inspector (BETA)
- BIND 9 DNS Cache Poisoning
- Patching the Holes in AJAX Security
- You Know about XSS. How about XSRF/CSRF?
- SCADA Honeynets
- Malware Removal Starter Kit
- Geographic Implications of DNS Infrastructure Distribution

---

### CCIP Contact Details:

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

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

## Security not a Benefit of Virtualisation

*Techworld*

Security has been touted as one of the benign by-products of virtualisation – but according to a recent study, that's no longer the case.

This is because technological developments mean malware can detect that it's running inside a VM and so alter its approach. Hiding the existence of a VM is "fundamentally infeasible," says the report, in response to the moaning by some virtualisation and security developers of the desirability of developing undetectable VMs.

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

## Secunia Personal Software Inspector (BETA)

*Secunia*

The Secunia PSI detects installed software and categorises your software as either Insecure, End-of-Life, or Up-To-Date. Effectively enabling you to focus your attention on software installations where more secure versions are available from the vendors.

Needless to say, we are very excited about this new free service for the Secunia security community. We appreciate all feedback, thoughts, and ideas that you wish to share with us.

Source: <https://psi.secunia.com/>

## BIND 9 DNS Cache Poisoning

*Amit Klein*

The paper shows that BIND 9 DNS queries are predictable – i.e. that the source UDP port and DNS transaction ID can be effectively predicted. A predictability algorithm is described that, in optimal conditions, provides very few guesses for the "next" query (10 in the basic attack, and 1 in the advanced attack), thereby overcoming whatever protection offered by the transaction ID mechanism. This enables a much more effective DNS cache poisoning than the currently known attacks against BIND 9. The net effect is that pharming attacks are feasible against BIND 9 caching DNS servers, without the need to directly attack neither DNS servers nor clients (PCs). The results are applicable to all BIND 9 releases, when BIND (the named daemon) is in caching DNS server configuration.

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

## Patching the Holes in AJAX Security

*SPI Dynamics*

Asynchronous JavaScript and XML technologies have taken the Web by storm. The popularity of the AJAX technique for building Web UI is growing at a tremendous rate and shows no sign of stopping. It isn't hard to understand why—AJAX applications can provide a much richer and more intuitive user interface than their traditional page-based counterparts.

However, AJAX is far from secure, and the decision to "AJAXify" a Web application shouldn't be made lightly. It demands that serious security implications be addressed across all phases of the application development life cycle.

Source: <http://www.spidynamics.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)

## You Know about XSS. How about XSRF/CSRF?

*Internet Storm Centre*

You know about cross-site scripting (XSS). It's an attack that injects malicious code into a vulnerable application such that the code executes in the victim's application viewer and, therefore, with the victim's session privileges. In most cases, the viewer is a web browser and the malicious code is written in JavaScript. (XSS won over the arguably more correct abbreviation "CSS" because of confusions with an unrelated term Cascading Style Sheets.)

Source: <http://isc.sans.org/>

## SCADA Honeynets

*By Dale Peterson*

A successful cyber attack on the SCADA (supervisory control and data acquisition) and other control systems that monitor and control electric grid, chemical plant or other critical infrastructure components could be massive in cost and potentially in loss of life. The SCADA security community is beginning to understand the vulnerabilities in control systems, a frightening topic.

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

## Malware Removal Starter Kit

*Microsoft*

Many small- and medium-sized organizations use antivirus software, and yet new viruses, worms, and other forms of malicious software (malware) continue to infect large numbers of computers in these organizations. Malware proliferates at alarming speed and in many different ways, which makes it particularly widespread today.

This guide is intended for IT Generalists who want information and recommendations that they can use to effectively address and limit malware that infects computers in small- and medium-sized organizations. This guidance provides a set of tasks that licensed Windows® users can perform at no cost to create the Malware Removal Starter Kit. Recommendations for free malware-scanning tools are included. You can use these tools in combination with the kit to conduct scans, detect problems, and remove malware from your computer.

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

## Geographic Implications of DNS Infrastructure Distribution

*Steve Gibbard, Packet Clearing House*

The past several years have seen significant efforts to keep local Internet communications local in places far from the well-connected core of the Internet. Although considerable work remains to be done, Internet traffic now stays local in many places where it once would have traveled to other continents, lowering costs while improving performance and reliability. Data sent directly between users in those areas no longer leaves the region. Applications and services have become more localized as well, not only lowering costs but keeping those services available at times when the region's connectivity to the outside world has been disrupted. I discussed the need for localization in a previous paper, "Internet Mini-Cores: Local connectivity in the Internet's spur regions." [1] What follows here is a more specific look at a particular application, the Domain Name System (DNS).

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



*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.*