

## Issue 92

Publication date: 14/01/2010

### Contents

- The WASC Threat Classification v2.0
- Identifying Key Practices for Secure Adoption of Cloud Computing
- Walowdac – Analysis of a Peer-to-Peer Botnet
- 2009 Data Breach Investigations Supplemental Report
- Cisco 2009 Annual Security Report
- How to steal a virtual machine and its data in 3 easy steps
- SCADA Enhancements for Snort; Part 1
- The Dark Side of the Smart Grid - Smart Meters (in) Security

### 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/>

## The WASC Threat Classification v2.0

*The Web Application Security Consortium*

The WASC Threat Classification is a cooperative effort to clarify and organize the threats to the security of a web site. The members of the Web Application Security Consortium have created this project to develop and promote industry standard terminology for describing these issues. Application developers, security professionals, software vendors, and compliance auditors will have the ability to access a consistent language and definitions for web security related issues.

Source: <http://projects.webappsec.org/>

## Identifying Key Practices for Secure Adoption of Cloud Computing

*Cloud Security Alliance*

The Cloud Security Alliance (CSA) today issued the second version of its “Guidance for Critical Areas of Focus in Cloud Computing”, now available on the Cloud Security Alliance website. The whitepaper, “Guidance for Critical Areas of Focus in Cloud Computing – Version 2.1”, outlines key issues and provides advice for both Cloud Computing customers and providers within 13 strategic domains. Version 2.1 provides more concise and actionable guidance across all domains, and encompasses knowledge gained from real world deployments over the past six months in this fast moving area.

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

## Walowdac – Analysis of a Peer-to-Peer Botnet

*honeyblog*

A botnet is a network of compromised machines under the control of an attacker. Botnets are the driving force behind several misuses on the Internet, for example spam mails or automated identity theft. In this paper, we study the most prevalent peer-to-peer botnet in 2009: Waledac. We present our infiltration of the Waledac botnet, which can be seen as the successor of the Storm Worm botnet.

Source: <http://honeyblog.org/>

## 2009 Data Breach Investigations Supplemental Report

*Verizon*

Verizon Business released the 2009 Data Breach Investigations Supplemental Report today. As you may know, the supplemental report addresses requests, issues, and questions that arise from our readers regarding the annual Data Breach Investigations Report (April, 2009). This year’s model is a catalogue of attacks that occurred most frequently in the data set used for the 2009 DBIR. It is, in large part, a divergence from previous reports in that it provides a more in-depth and wider view of a data breach, and is not solely statistics driven. The aim of the report is to provide both technical personnel and managers with a one-stop compendium of pertinent details on the widespread threats within our caseload. It is our hope that readers can directly utilize the information provided to prepare for, detect and, ideally, prevent these types of attacks.

Source: <http://securityblog.verizonbusiness.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

CCIP Security Guidelines

NetSafe

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

## Cisco 2009 Annual Security Report

*Cisco*

Cisco Security Intelligence Operations announces the Cisco 2009 Annual Security Report. The updated report includes information about 2009 global threats and trends, as well as security recommendations for 2010. Managing and securing today's distributed and agile network is increasingly challenging, with cloud computing and sharing of data threatening security norms. Online criminals are continuing to exploit users trust in consumer applications and devices, increasing the risk to organizations and employees.

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

## How to steal a virtual machine and its data in 3 easy steps

*SearchVMware.com*

Remember the email server or payroll system that you virtualized? Someone with administrator access to your virtual environment could easily swipe it and all the data without anybody knowing. Stealing a physical server out of a data center is very difficult and is sure to be noticed, stealing a virtual machine (VM), however, can be done from anywhere on your network, and someone could easily walk out with it on a flash drive in their pocket.

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

## SCADA Enhancements for Snort; Part 1

*Digital Bond*

In mid-December we completed the Quickdraw project which creates security events for legacy PLC's that lack a security event logging capability. In the following weeks I will write a blog series on Quickdraw, but a lot of this work involves adding SCADA preprocessors and plugins to Snort. So let's start with a SCADA Snort blog series. While these were necessary and valuable for Quickdraw, they also will be very helpful for IDS/IPS and may play a role in adding deep inspection to field firewalls.

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

## The Dark Side of the Smart Grid - Smart Meters (in)Security

*C4 Security*

This whitepaper will first demonstrate why Smart Grid technologies pose a complex yet critical security issue for the utility adopting it. Following the demonstration of the need to secure the Smart Grid, 9 critical attack vectors and vulnerabilities relevant to Smart Grid deployments will be presented. These scenarios are investigated for two main reasons:

- 1. Raise the security awareness regarding the new threats introduced by implementing a Smart Grid
- 2. Encourage a discussion about potential remedies to mitigate these vulnerabilities

The information and vulnerabilities mentioned in this whitepaper are a result of security audits performed by C4 Security on 3 Smart Grid deployments – one for a water pipeline utility and two for electric grids.

Source: <http://www.c4-security.com/> (pdf)

*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.*

