

## Issue 84

Publication date: 02/09/2009

### Contents

- Twenty Critical Controls for Effective Cyber Defense: Consensus Audit
- GNSO Fast Flux Hosting Working Group Publishes Final Report
- Protecting Against Insider Attacks
- The End of Domain Tasting
- The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained
- The Scale of Security
- Flash Cookies and Privacy
- Network Capture Tools and Utilities
- Publicly Available PCAP Files

### 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/>

## Twenty Critical Controls for Effective Cyber Defense: Consensus Audit

*SANS Institute*

Securing our nation against cyber attacks has become one of the nation's highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against a variety of threats, both internal and external. Furthermore, for those attacks that are successful, defenses must be capable of detecting, thwarting, and responding to follow-on attacks on internal enterprise networks as attackers spread inside a compromised network.

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

## GNSO Fast Flux Hosting Working Group Publishes Final Report

*ICANN*

In May 2008, the GNSO Council launched a Policy Development Process (PDP) that tasked a Working Group to answer a number of questions related to fast flux hosting. Fast flux hosting is a technique that utilizes short Time To Live settings and frequent updates of DNS records to increase a domain's resiliency. It has legitimate uses, but is widely known as a tactic cybercriminals use to enhance their phishing and pharming gains.

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

## Protecting Against Insider Attacks

*SANS Reading Room (Brad Ruppert)*

This paper will discuss the key factors in helping to enhance security to protect a company from internal attacks. Most companies focus their resources and defensive strategies on protecting the perimeter from outsider attacks but often the greatest damage can be done by someone already inside these defenses. System administrators can be a company's most trusted ally or their worst nightmare depending on their motivation or personal interest. It is imperative that companies implement internal controls to monitor, detect, and prevent access to sensitive resources to only those individuals that require it to perform their specific job function. The goal of this paper will be to identify high risk areas commonly neglected and to provide some best practice tips to enhance internal security controls.

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

## The End of Domain Tasting

*ICANN*

A report released today by ICANN shows that the so-called practice of "Domain Tasting," has all but been eliminated as a result of a solution developed only one year ago. At its peak, the practice of speculatively registering domain names for very short periods of time (less than 5 days) saw millions of dot-com domains, as one example, registered and returned in one month alone. However, following recent policy changes by ICANN after extensive consultations with the Internet community, there has been a 99.7% decline in domain tasting across all registries that have implemented the new domain tasting policy, according to the new ICANN report.

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

### 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)

## The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained

*Trend Micro Threat Research*

KOOBFACE is a revolutionary malware, being the first to have a successful and continuous run propagating through social networks. Its success can, unfortunately, set a precedent for other malware families to abuse social networking sites. In this paper, we attempt to dissect KOOBFACE by component in order to allow users to understand what the KOOBFACE threat is and what it does.

Source: <http://us.trendmicro.com/>

## The Scale of Security

*SecurityFocus*

Human beings do not naturally understand scale. While we speak of financial transactions in the hundreds of billions of dollars as being something as routine as brushing our teeth, we question the value of programs that cost in the single-digit millions and quibble with friends over dollars. Similarly, there are many problems in our industry that, when explained to an outsider, sound like they should have been solved decades ago. It is only when we relate the number of systems that need to be considered in the repair that we truly communicate the difficulty of the problem.

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

## Flash Cookies and Privacy

*Social Science Research Network*

This is a pilot study of the use of 'Flash cookies' by popular websites. We find that more than 50% of the sites in our sample are using flash cookies to store information about the user. Some are using it to 'respawn' or re-instantiate HTTP cookies deleted by the user. Flash cookies often share the same values as HTTP cookies, and are even used on government websites to assign unique values to users. Privacy policies rarely disclose the presence of Flash cookies, and user controls for effectuating privacy preferences are lacking.

Source: <http://papers.ssrn.com/>

## Network Capture Tools and Utilities

*Grand Stream Dreams blog*

At a conference this week, we had quite a section regarding network captures. The instructor was going on about how you can try to sort out users and what they are doing via Wireshark with the packet captures. He was really wanting to figure out who the largest users were and what they were doing to saturate the bandwidth. I politely asked if he was familiar with NetworkMiner Network Forensic Analysis Tool (NFAT) and Packet Sniffer. He was not. So I asked if I could come up and demo the one I had stowed on my USB stick.

Source: <http://grandstreamdreams.blogspot.com/>

## Publicly Available PCAP Files

*SourceForge, Inc.*

This is a directory over various packet capture repositories which are freely and publicly available on the Internet. Most of the sites listed below share their PCAP files as full content, but some do unfortunately only have truncated frames.

Source: <http://sourceforge.net/>



*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.*

