

Issue 40

Publication date: 22/06/07

Contents

- CERT's Resiliency Engineering Research
- OPERATION: BOT ROAST - 'Bot-herders' Charged
- February 2007 Root Server Attacks - A Qualitative Report
- Implementing an Effective Security Strategy
- Security Analogies Wiki
- Security Hacks
- Issues in Using DNS Whois Data for Phishing Site Take Down
- What is Social Engineering?

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/>

CERT's Resiliency Engineering Research

CERT/CC

The CERT® Resiliency Engineering Framework... is the foundation for a process improvement approach to security and business continuity. It establishes an organization's resiliency engineering process: a collection of essential capabilities that an organization performs to ensure that its important assets—people, information, technology, and facilities—stay productive in supporting business processes and services. The framework serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security and business continuity activities and takes on a process improvement mindset that helps to keep these activities productive in the long run.

Source: http://www.cert.org/resiliency_engineering/

OPERATION: BOT ROAST - 'Bot-herders' Charged

Federal Bureau of Investigation

They're called "bot-herders:" hackers who install malicious software on computers through the Internet without the owners' knowledge. Once the software is loaded, they can control the computer remotely. And once they've compromised enough computers, they have a robot network or botnet.

As a result of Operation Bot Roast, an ongoing and coordinated initiative to disrupt and dismantle these bot-herders, we've identified about 1 million computers across the country that have been compromised.

Source: <http://www.fbi.gov/page2/june07/botnet061307.htm>

February 2007 Root Server Attacks - A Qualitative Report

Arbor Networks

During the ISP Security BOF at NANOG 40 last week in Bellevue, Washington, John Kristoff of Neustar Ultra Services provided a nice summary of what actually occurred during the February 6/7, 2007 DNS attacks.

He began by providing a summary of the considerable amount of mis-information provided about the attacks, with his personal favorite being an article titled UltraDNS attack targeted G and L root servers (1st Update). I suppose I can see how such a title might prove a bit misleading. From there, John noted some of the more useful information provided at the time, and in particular that from a lightning talk at NANOG 39 by Dave Knight at the tail end of the attacks.

Source: <http://asert.arbornetworks.com/2007/06/february-2007-root-server-attacks-a-qualitative-report/>

Implementing an Effective Security Strategy

Security Park

In the last ten years, the risks for enterprise security have grown steadily and new types of attacks have appeared. These are often combinations of viruses, Trojans or other malware from a wide range of anonymous sources. At the same time, enterprise networks are growing ever more complex. A large number of servers are dedicated to a variety of tasks, while virtualisation combines multiple systems into one – and compliance with legal requirements must simultaneously be assured.

Source: <http://www.securitypark.co.uk/article.asp?articleid=27050&CategoryId=1>

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)

Security Analogies Wiki

Security Analogies

This site is dedicated to compiling good analogies used when explaining (computer) security matters. One of the challenges security experts face is expressing in simple language the issues involved in security. Analogies are often a good way of making plain what the issues are, in a language that is easy to understand. Of course, analogies have their problems; this wiki will hopefully allow us to fine-tune the analogies to make them as close a match as possible.

Source: http://www.securityanalogies.com/index.php/Main_Page

Security Hacks

Security-Hacks.com

Security-Hacks.com was opened as a website dedicated to covering tips and tricks related to security. Whether it is an interesting utility, or just a cool configuration option in Windows/Linux/Mac, we will cover it. We focus mostly on pointing out tools for download — mostly freeware/opensource — and writing up quick how-to's and tutorials.

Security-Hacks is updated several times daily by a group of people who do research in security as a hobby or job who wanted a place for people to find little tidbits of information. Since this site is targeted towards interesting and helping you, we will be more than glad to hear any suggestions for improvements, or article requests.

Source: <http://www.security-hacks.com/>

Issues in Using DNS Whois Data for Phishing Site Taken Down

Anti-Phishing Working Group

Given fundamental policy changes regarding accessibility of Whois data currently under consideration by ICANN, and the evolving environment surrounding the Whois system, the APWG DNS Subcommittee has produced this industrial advisory, comprised of a set of real-world case studies in which Whois data has been instrumental in neutralizing phish sites, to help ICANN comprehensively inform these policy deliberations. The intent is to better inform the broader ICANN community of the invaluable assistance the full range of Whois data provides in shutting down nearly 1,000 phishing sites per day (and climbing) at current rates. Each of these cases considered describes a specific event, but represents hundreds of analogous events that occur daily.

Source: http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf

What is Social Engineering?

SecureWorks

Social engineering is described as a collection of primarily non-technical intrusion techniques used to manipulate other people. Basically, social engineering is a new version of an age old con game that relies heavily on human interaction to break normal security procedures (fraud). Though any organization can be susceptible to the con, social engineers usually target larger entities including financial institutions, government institutions, and hospitals.

Source: <http://www.secureworks.com/research/newsletter/2007/06/#social>



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.