



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE *for* CRITICAL INFRASTRUCTURE PROTECTION

Issue 85

Publication date: 16/09/2009

Contents

- The Top Cyber Security Risks - Two risks dwarf all others, but organizations fail to mitigate them
- A Cybercrime Hub
- Shedding Light on the Dark Cyber World
- Network Capture Tools and Utilities
- The state of malicious internet activity
- Pushing Boulders Uphill: The Difficulty of Network Intrusion Recovery
- Recommendations for the Remediation of Bots in Large ISP Networks
- Schneier-Ranum Face-Off: Is Perfect Access Control Possible?

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/>

The Top Cyber Security Risks - Two risks dwarf all others, but organizations fail to mitigate them

SANS Institute

Throughout the developed world, governments, defense industries, and companies in finance, power, and telecommunications are increasingly targeted by overlapping surges of cyber attacks from criminals and nation-states seeking economic or military advantage. The number of attacks is now so large and their sophistication so great, that many organizations are having trouble determining which new threats and vulnerabilities pose the greatest risk and how resources should be allocated to ensure that the most probable and damaging attacks are dealt with first. Exacerbating the problem is that most organizations do not have an Internet-wide view of the attacks.

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

A Cybercrime Hub

Trend Micro

Tartu, Estonia is the hometown of an Internet company that, from the outside, looks just like any other legitimate Internet service provider (ISP). On its website, the company lists services such as hosting and advertising. According to publicly available information, it posted more than US\$5 million in revenue and had more than 50 employees in 2007.

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

Shedding Light on the Dark Cyber World

Converge! Media Ventures, Inc.

Global electronic networks of increasing power and pervasiveness form the communications backbone of this 21st century world economy, just as railroads, steamships, telegraphs and postal systems formed the transportation and communications infrastructure of the 19th century industrial economies. The foundation for the creation of the new digital era, also referred to as cyber world, virtual world or digital world, is the rapid and effective deployment of information and communication technologies in all sectors of our lives, ranging from economy, government and businesses to consumers at large.

Source: <http://www.convergedigest.com/> (Part I)

<http://www.convergedigest.com/> (Part II)

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/>

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 state of malicious internet activity

CIO Magazine

The effects of cybercrime are far reaching. It would be a difficult task to find someone who has never been affected by malicious internet activity, or who does not at the very least know someone who has been negatively impacted by cybercriminals. Advances in internet technology and services continue to open up innumerable opportunities for learning, networking and increasing productivity. However, malware authors, spammers and phishers are also rapidly adopting new and varied attack vectors. If the internet is to become a safer place, it is imperative to understand the trends and developments taking place in the internet threat landscape and maintain online security best practices.

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

Pushing Boulders Uphill: The Difficulty of Network Intrusion Recovery

Michael e. Locasto, Matthew Burnside, Darrell Bethea

We present a study of three significant compromises of a medium-scale network infrastructure. We do so as a way to expose the difficulties - both technical and human - inherent in intrusion recovery. Most network users take a "secure" network infrastructure for granted. Real events show that this level of faith is unwarranted, as is the belief that intrusions are or can be completely repaired, especially in the absence of research on network recovery mechanisms that explicitly take the needs of support staff into account.

Source: <http://www.cs.gmu.edu/> (pdf)

Recommendations for the Remediation of Bots in Large ISP Networks

Internet Engineering Task Force

This document contains recommendations on how large Internet Service Providers (ISPs) can manage the effects of large numbers of bot infected computers used by their subscribers via various remediation techniques. At the time that this document was published, computers infected by bots and the users of those computers comprise a substantial number of users for large ISPs. Those Internet users are exposed to risks such as loss of personal data, increased susceptibility to online fraud and/or phishing, and becoming an inadvertent participant in or component of an online crime, spam, and/or phishing network. Mitigating the effects of and remediating the installations of bots affecting large numbers of Internet users will make it more difficult for botnets to operate and could reduce the level of online crime on the Internet in general and/or on a particular ISP's network.....'

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

Schneier-Ranum Face-Off: Is Perfect Access Control Possible?

SearchSecurity

Access control is difficult in an organizational setting. On one hand, every employee needs enough access to do his job. On the other hand, every time you give an employee more access, there's more risk: he could abuse that access, or lose information he has access to, or be socially engineered into giving that access to a malfeasant. So a smart, risk-conscious organization will give each employee the exact level of access he needs to do his job, and no more.

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

