

Issue 89

Publication date: 13/11/2009

Contents

- ICCP Technology Foresight Forum - "Cloud Computing: The Next Computing Paradigm?"
- Layer 2 Network Protections against Man in the Middle Attacks
- The Four Myths of Cyber Security
- Inside Trojan.Clampi: The Research Paper
- Phishing Activity Trends Report, 1st Half / 2009
- Microsoft Baseline Security Analyzer 2.1
- The Seven Deadly Sins of Security Policy
- A New Milestone for Microsoft
- Windows 7 will Slash Malware

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/>

ICCP Technology Foresight Forum - "Cloud Computing: The Next Computing Paradigm?"

OECD

In 2008 the term "cloud computing" became fashionable as a way to refer to a number of interlinked information technology trends. There are a number of competing interpretations of what cloud computing is about, but in its simplest formulation the expression refers to the provision of computing resources at a distance, over the Internet. This would hardly seem to be a novel concept, and indeed it harkens back in some respects to the early days of computing with big mainframes doing the computing work for remote users at work stations. Yet the term is suggestive of important shifts in IT, which may bring economic, policy and possibly regulatory implications.

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

Layer 2 Network Protections against Man in the Middle Attacks

Internet Storm Centre

Last month (Day 9 of Cyber Security Awareness Month) we discussed a Man in the Middle (MITM) attack against RDP (Microsoft's Remote Desktop Protocol), along with Man in the Middle protections for RDP services. The article and video illustrate the just how easy it is to mount a man in the middle attack using ARP cache poisoning. We've also recently covered recent research in SSL Man in the Middle vulnerabilities and this month's issues concerning MITM attacks against TLS renegotiation. Today's entry discusses network protections that provide mitigation for all services against such attacks (not just a specific protocol or vulnerability). We'll be discussing mitigations that can be applied in most corporate settings (Private VLANs aren't covered).

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

The Four Myths of Cyber Security

BusinessComputingWorld

Incidents and exploits crafted by an effective and growing menace are threatening the continuity of, and confidence in, the very core of our commercial and social infrastructure. In just 90 criminal investigations performed in 2008, where data compromise was confirmed, the Verizon Business RISK team (a leading computer forensics group) reported more than 285 million consumer credit records stolen. This number far exceeds the combined total confirmed for all their investigations from 2004 to 2007.

Source: <http://www.businesscomputingworld.co.uk/>

Inside Trojan.Clampi: The Research Paper

Symantec

Trojan.Clampi is an interesting threat, which we described in many blog entries over the past month. In a nutshell, Clampi is an Infostealer threat. Its executable can be seen as a host for separate modules, containing the real payloads of the threat. These modules are heavily protected from reverse-engineering as well. The functionalities range from banking-site password stealing, to local credential gathering, to a SOCKS proxy. The communication with Clampi's command & control servers, the "Gates", uses HTTP and is encrypted. Clampi spawns and uses an Internet Explorer instance as an API proxy to achieve network communication, bypassing firewalls along the way.

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

Phishing Activity Trends Report, 1st Half / 2009

Anti-Phishing Working Group (APWG)

The quarterly APWG Phishing Activity Trends Report analyzes phishing attacks reported to the APWG by its member companies, its Global Research Partners, through the organization's website at <http://www.antiphishing.org> and by email submissions to reportphishing@antiphishing.org. APWG also measures the evolution, proliferation and propagation of crimeware drawing from the research of our member companies. In the last half of this report you will find tabulations of crimeware statistics and related analyses.

Source: <http://www.antiphishing.org/> (pdf)

Microsoft Baseline Security Analyzer 2.1

Microsoft

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. Improve your security management process by using MBSA to detect common security misconfigurations and missing security updates on your computer systems.

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

The Seven Deadly Sins of Security Policy

NetworkWorld

In today's compliance-centric world, your organization may have so many security policies that you've lost track. But how effective are your policies at really mitigating the risks you face? And are there some that you might have put in place simply to follow the law but that just aren't being enforced? According to the policy experts we interviewed, those are just two of the several common mistakes an organization can make when putting policies on the books.

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

A New Milestone for Microsoft

Emagined Security

We all know what "Patch Tuesday" is. Every month on the second Tuesday, Microsoft releases a bulletin describing vulnerabilities and hot fixes or descriptions of workarounds in its products. Interestingly, six years have now gone by between the time of the first Patch Tuesday and the one two days ago. Over these six years, Microsoft has distributed nearly 400 bulletins that have described nearly 750 vulnerabilities. Most of these vulnerabilities have not been trivial, either; Microsoft has in fact rated over half of these vulnerabilities as "critical."

Source: <http://blog.emagined.com/>

Windows 7 will Slash Malware

CIO Magazine

Microsoft caused the IT security community more than a little heartburn when it included fixes for the barely-out-of-the-box Windows 7 in its October 2009 Patch Tuesday security update. Nevertheless, Jimmy Kuo - principal architect for Microsoft's Malware Protection Center - has high hopes that Windows 7 will ultimately be seen as the major turning point where malware writers finally met their match.

Source: <http://cio.co.nz/> | <http://www.microsoft.com/> (latest SIR Report)

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.

