

Issue 94

Publication date: 25/03/2010

Contents

- Malware Attribute Enumeration and Characterization
- Underrated Computing Threats you Need to Know About
- How a Process Model can Help Bring Security into Software Development
- Top Threats to Cloud Computing
- An Introduction to Virtualization Security
- Public Comment: Draft Report on WHOIS Accuracy
- Jericho Self-Assessment Scheme
- AS-Troyak Exposes a Large Cybercrime Infrastructure

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/>

Malware Attribute Enumeration and Characterization

Mitre

Malware Attribute Enumeration and Characterization (MAEC™) is a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns. By eliminating the ambiguity and inaccuracy that currently exists in malware descriptions and by reducing reliance on signatures, MAEC aims to improve human-to-human, human-to-tool, tool-to-tool, and tool-to-human communication about malware; reduce potential duplication of malware analysis efforts by researchers; and allow for the faster development of countermeasures by enabling the ability to leverage responses to previously observed malware instances.

Source: <http://maec.mitre.org/>

Underrated Computing Threats you Need to Know About

NetworkWorld

There's the danger you know, and then there's the danger you don't know. Most of us are rightfully wary of downloading and running programs that have no pedigree, or of performing day-to-day operations as an administrative user. But with each passing year, new security threats march in to eclipse the old -- many of them not getting their share of attention until it's too late. Threats go unappreciated for various reasons. Some seem too obscure or unlikely to be valid until they actually materialize in the wild (such as the .PDF exploits I document later on). Others are overshadowed by more widely publicized problems

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

How a Process Model can Help Bring Security into Software Development

Government Computing News

Lifecycle processes have been around for years, so why has it been so difficult to incorporate security into the process? The secure software development lifecycle (sSDLC) comprises a number of complex processes that require early involvement by business users, project managers and applications developers, as well as information security practitioners, to successfully develop a functional and secure product. An organization must adopt a process model wherein process improvements are managed from a common framework.

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

Top Threats to Cloud Computing

Cloud Security Alliance

The purpose of this document, Top Threats to Cloud Computing, is to provide needed context to assist organizations in making educated risk management decisions regarding their cloud adoption strategies. In essence, this threat research document should be seen as a companion to Security Guidance for Critical Areas in Cloud Computing. As the first deliverable in the CSA's Cloud Threat Initiative, the "Top Threats" document will be updated regularly to reflect expert consensus on the probable threats which customers should be concerned about.

Source: <http://cloudsecurityalliance.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)

An Introduction to Virtualization Security

Help Net Security

Virtualization platforms are software. All software has flaws. Therefore, virtualization platforms have flaws. Simple logic, right? The major virtualization platform vendors, VMware, Xen (now Citrix), and Microsoft, have all had several vulnerabilities over the last few years. However, the major components of a virtualization infrastructure and the IT strategy related to deployment and maintenance of virtualization technologies can be planned and secured fairly well. The following sections will explore the major areas of concern for security professionals.

Source: <http://www.net-security.org/>

Public Comment: Draft Report on WHOIS Accuracy

ICANN

The National Opinion Research Center (NORC) recently completed a study commissioned by ICANN to determine the percentage of domain names registered under the top 5 gTLDs (i.e., .com, .net, .org, .biz, and .info) that contain accurate WHOIS data. Today, the draft report is being posted for review and comment through 15 April 2010. Community members are invited to review the draft report and its findings and comment on all aspects of the report. The information in the report is intended to contribute to the ongoing community discussion regarding WHOIS and should be useful in any future policy development process regarding WHOIS.

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

Jericho Self-Assessment Scheme

The Open Group

On March 15th 2010 the Jericho Forum launched its Self-Assessment Scheme (SAS), a new tool that will allow vendors and their customers to check the effectiveness of an IT security product in meeting their needs, particularly as more organizations adopt cloud computing. The scheme provides security vendors with a high-value, free-of-charge tool to assess how well a solution satisfies the requirements mandated in the Jericho Forum Commandments - the eleven principles of good security design established by the forum in 2006.

Source: <https://www.opengroup.org/>

AS-Troyak Exposes a Large Cybercrime Infrastructure

RSA Security

Last week, RSA and other security professionals noticed a sudden halt in the activity of an upstream Internet connectivity provider named "AS-Troyak", thus causing several major malware-hosting networks to disconnect from the Internet. Further investigation proved that AS-Troyak is merely one part of a larger cybercrime infrastructure providing "bulletproof" hosting to malicious content perpetrators.

Source: <http://www.rsa.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.

