

Issue 87

Publication date: 15/10/2009

Contents

- Release of Interisle and TNO reports on Root Scaling
- Conficker C P2P Protocol and Implementation
- Navigating the New Cybercrime Threatscape, Part 1
- DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies
- The Beating Heart of Banking: Insights into Global Payments
- Guidelines on Firewalls and Firewall Policy
- MessageLabs Intelligence: Q3/September 2009
- How to Deploy NetFlow v5 and v9 Probes and Analyzers
- The Heart of KOOBFACE: C&C and Social Network Propagation

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/>

Release of Interisle and TNO reports on Root Scaling

ICANN

In February 2009, with Resolution 2009-02-03-04, the ICANN Board requested the Root Server System Advisory Committee (RSSAC), the Security and Stability Advisory Committee (SSAC), and the ICANN staff, including the IANA team, to study the potential issues regarding the addition of IDNs, IPv6 addresses, DNSSEC and substantial numbers of new TLDs to the root zone.

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

Conficker C P2P Protocol and Implementation

SRI International

This report presents a reverse engineering of the obfuscated binary code image of the Conficker C peer-to-peer (P2P) service, captured on 5 March 2009 (UTC). The P2P service implements the functions necessary to bootstrap an infected host into the Conficker P2P network through scan-based peer discovery, and allows peers to share and spawn new binary logic directly into the currently running Conficker C process. Conficker's P2P logic and implementation are dissected and presented in source code form. The report documents its thread architecture, presents the P2P message structure and exchange protocol, and describes the major functional elements of this module.

Source: <http://mtc.sri.com/>

Navigating the New Cybercrime Threatscape

TechNewsWorld

It didn't take long for criminals to realize the potential that the Internet had as a vehicle for fraud, deception and theft. Malware like viruses and worms quickly evolved from annoying bits of code that did little actual harm into methods used to rip off the unwitting.

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

DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies

National Institute of Standards and Technology

NIST announces the public comment release of draft SP 800-127, Guide to Security for WiMAX Technologies. Worldwide Interoperability for Microwave Access (WiMAX) is a wireless metropolitan area network communications technology based on the IEEE 802.16 standard. WiMAX technologies were originally developed to provide last-mile broadband wireless access, but are now more focused on cellular-like mobile architectures. Draft SP 800-127 explains the basics of WiMAX, provides information on the security capabilities of WiMAX, and gives recommendations on securing WiMAX technologies effectively. It also explains the security differences among the major versions of the IEEE 802.16 standard

Source: <http://csrc.nist.gov/>

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 Beating Heart of Banking: Insights into Global Payments

KPMG

The results of an early 2009 survey showing a range of views from industry regulators, major banks and financial technology companies about the factors they believed would drive future change in the global payments industry. This report offers an overview of current issues and trends in payments, ranging from efficiencies in payment systems to new technology, systemic risk and evolving business models.

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

Guidelines on Firewalls and Firewall Policy

National Institute of Standards and Technology

NIST announces the release of Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy. It provides recommendations on developing firewall policies and on selecting, configuring, testing, deploying, and managing firewalls. The publication covers a number of firewall technologies, including packet filtering, stateful inspection, application-proxy gateways, host-based, and personal firewalls. SP 800-41 Revision 1 updates the original publication, which was released in 2002.

Source: <http://csrc.nist.gov/>

MessageLabs Intelligence: Q3/September 2009

MessageLabs

Latest Investigation of Spam from Botnets Reveals Rapid Growth; Rustock's Heartbeat, Maazben Gambles to Dominate and Grum Becomes Worst Offender

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

How to Deploy NetFlow v5 and v9 Probes and Analyzers

Richard Bejtlich

Session data is one of the six kinds of network security monitoring (NSM) data available to detect and respond to intrusions, and for troubleshooting, measuring and operating your customers' networks. (The other forms of NSM data are alert, full content, statistical, transaction, and extracted content.) NetFlow is Cisco's preferred method for providing session data, although the open source community has software to generate and collect NetFlow records as well. In this article I will demonstrate how to deploy an open source NetFlow probe and an open source NetFlow collector, as well as briefly describe and compare NetFlow v5 and v9.

Source: <http://searchnetworkingchannel.techtarget.com/>

The Heart of KOOBFACE: C&C and Social Network Propagation

Trend Micro

This is the second part of the three-part paper by Trend Micro Threat Researchers Jonell Baltazar, Joey Costoya and Ryan Flores discussing the KOOBFACE botnet in more technical detail and chronicling the behavior and payloads of each component.

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

