

Issue 42

Publication date: 23/07/07

Contents

- When Spambots Attack — Each Other!
- CIS Benchmarks
- How to Conduct Firewall Configuration Reviews
- Phishing under the Microscope
- Global Security Week 2007: “Privacy in the 21st Century”
- High Volume of Email Linking to the “Storm Worm” Malware
- Know Your Enemy: Fast-Flux Service Networks
- Shoring up your Framework
- Employees Pose Biggest Cyber Security Risk
- X-Force Threat Insight Monthly

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/>

When Spambots Attack — Each Other!

Arbor Networks

So, you’ve read plenty about when botnets attack. You’ve also seen plenty about when spambots attack, though it’s usually only in the form of spam email flooding in the course of spambot offspring performing the functions for which their creator intended. There’s even been plenty of press about when Botnets Battle Over Turf, attacking each other. So, let’s delve into one example of why that is, and take a terse look at one such set of attacks.

Source: <http://asert.arbornetworks.com/>

CIS Benchmarks

Center for Internet Security

CIS Benchmarks enumerate security configuration settings and actions that “harden” your systems. They are unique, not because the settings and actions are unknown to any security specialist, but because consensus among hundreds of security professionals worldwide has defined these particular configurations.

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

How to Conduct Firewall Configuration Reviews

SearchSecurity.com/

Firewall configuration reviews play a critical role in ensuring the ongoing protection of the perimeter. As any firewall administrator knows, it’s all too easy for a rule base to become convoluted over time, containing rules that may be outdated or simply incorrect. Regular reviews help remedy this effect and allow administrators to conduct a periodic policy “health check.”

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

Phishing under the Microscope

IBM Internet Security Systems

When discussing phishing, most people I meet are only all-too familiar with the spam-based email flooding their inbox and the cloned websites waiting out there to suck down their banking credentials and steal their identity. But many of them have no inkling as to the mechanics and logistical challenges behind the attack.

Source: <http://blogs.iss.net/>

Global Security Week 2007: “Privacy in the 21st Century”

Global Security Week (GSW)

The 3rd annual Global Security Week will run from September 3rd to 9th 2007 with this year’s theme being “Privacy in the 21st Century”. The theme this year is intended to highlight how individuals and companies can better protect personal information that is not only stored online and on various different computer systems, such as mobile computing devices, portable storage devices, and multiple types of servers, but also on printed paper as well as through discussions about confidential matters in public locations, and any other way in which personal information is stored or shared.

Source: <http://www.globalsecurityweek.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

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)

High Volume of Email Linking to the “Storm Worm” Malware

AusCERT

AusCERT has observed very large amounts of email purporting to be greeting cards and security updates containing links to malware. This malware is a variant of what is widely known as the “Storm worm”, but also known as Tibs or Peacomm.

Source: <http://www.auscert.org.au/>

Know Your Enemy: Fast-Flux Service Networks

The Honeynet Project & Research Alliance

One of the most active threats we face today on the Internet is cyber-crime. Increasingly capable criminals are constantly developing more sophisticated means of profiting from online criminal activity. This paper demonstrates a growing, sophisticated technique called fast-flux service networks which we are seeing increasingly used in the wild. Fast-flux service networks are a network of compromised computer systems with public DNS records that are constantly changing, in some cases every few minutes. These constantly changing architectures make it much more difficult to track down criminal activities and shut down their operations.

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

Shoring up your Framework

IT Compliance Institute

No single enterprise risk management framework is comprehensive enough to guide your company in meeting all of its compliance, governance, and risk management needs. Instead, you'll want to selectively combine standards by building around a central framework, such as COSO or AS/NZS 4360, and reinforcing it with one or more of these risk assessment standards.

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

Employees Pose Biggest Cyber Security Risk

DarkReading.com

Security Researcher Simple Nomad (aka Mark Loveless) explains how and why end users are the biggest issue in cyber security. “The problem is that you have a sophisticated attack vector, Windows, that they're all using, so you have commonality,” he said. “From an attacker's standpoint, it's great. If I develop a Windows exploit all I have to do is get one of these users to click on it.” “Whenever a box pops up on the screen, a user will click ‘OK’ because that makes the box go away,” he added.

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

X-Force Threat Insight Monthly

IBM Internet Security Systems

The first half of the July edition of the X-Force® Threat Insight Monthly discusses the Web Operating System (WebOS). As Web-based applications become more prolific and functional in the modern computing environment, the WebOS will become a viable alternative to the concept of a local platform. This expansion will continue to increase the attack surface against Web-based applications, with consequences yet to be understood.

Source: <http://www.iss.net/>



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.