CyberPro

Volume 1, Edition 2
June 9, 2008

Keeping Cyber Professionals Informed

This newsletter is intended to keep subscribers who are involved in the development of Cyber-related concepts and initiatives informed on items of common interest. The newsletter and the information contained therein shall not be used to provide a competitive advantage for any commercial firm. Any misuse or unauthorized use of the newsletter and its contents will result in removal from the distribution list and other appropriate administrative, civil, and/or criminal action.

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or National Security Cyberspace Institute.

To subscribe or unsubscribe to this newsletter click here CyberPro News Subscription.

Table of Contents

CyberPro

Volume 1, Edition 2
June 9, 2008

Keeping Cyber Professionals Informed

** CYBER-RELATED CONFERENCES **

Note: Dates and events change often. The following is unofficial. Contact POCs for details.

If you have any additions/updates/suggestions for the CYBER calendar of events, please provide them to Larry McKee at mckeel@selectinnovation.com

9-10 June 2008	**Cyber Security Conference - Missions, Initiatives, Opportunities & Risks**, Washington DC, http://www.asdevents.com/event.asp?ID=238
16-20 June 2008	**Cyber Security for Process Control Systems Summer School**, At the Abbey Resort on Lake Geneva, Fontana, Wisconsin, http://www.iti.uiuc.edu/events/SummerSchool2008.html
17-18 June 2008	Enterprise Security Management Spring Forum, Bellevue WA, www.afei.org
17-19 June 2008	**Joint Warfighting 2008, "DoD Capabilities for the 21st Century"**, Virginia Beach VA, http://www.afcea.org/events/east/08/intro.asp
17-19 June 2008	**Cyberspace Symposium II,** Marlborough MA, https://www.paulrevereafa.org/CyberSymposium/index.asp
23-25 June 2008	**Space Warfare Symposium, "Space Situation Awareness and Command and Control: Keys to Future Global Security in Space"**, Keystone, CO -- http://www.spacewarfare.org/
24-27 June 2008	**Information Operations Europe 2008**, London UK http://www.asdevents.com/event.asp?ID=215
26-27 June 2008	**Identity Assurance: Authentication, Protection, and Federation**, Ronald Reagan International Trade Center, Washington, D.C. http://www.afcea.org/events/register.cfm?ev=17
14-17 July 2008	**Annual International Test & Evaluation Association Technology Review**, Crowne Plaza Hotel, Colorado Springs CO, www.itea.org
15 – 17 July 2008	**Air Force Symposium 2008 – Cyberspace**, Maxwell AFB (Montgomery) AL www.maxwell.af.mil/au/awc/cyberspace
25 – 26 Sept 2008	**Electronic Warfare Operations and Systems 2008**, London UK, http://www.asdevents.com/event.asp?ID=241
6-8 October 2008	**Strategic Space & Defense**, Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/

***** OPEN-SOURCE MATERIAL *****

Malicious code makes Web surfing risky

GOVERNMENT COMPUTER NEWS
06/06/2008

McAfee Inc estimates that the risk of downloading malware online has increased 41% in the past year alone. The study, "Mapping the Web Revisited," suggests avoiding sites that end in .hk, which are the country domain for Hong Kong, as one in five sites on the domain were found to pose a security threat. McAfee summarizes that the web is becoming more dangerous altogether, although some parts of the web are riskier than others, primarily country domains for Hong Kong, China, the Philippines and Romania.
http://www.gcn.com/online/vol1_no1/46417-1.html

Computer Hack Could Lead to JDAM Strike

BY: CHRISTIAN LOWE, MILITARY.COM
06/05/2008

Col. Tony Buntyn explains that you can use the same terminology with kinetic warfare as you can with cyber warfare, and that hacking into a government system should be viewed the same as dropping an actual bomb. Cyber warfare is becoming an "increasingly critical capability" to the United States military, and nations such as China, Russia and North Korea have already discreetly entered the cyber-warfare arena. Buntyn explains that one major issue facing cyber-warfare is determining the level of our response to cyber attacks; determining whether a kinetic or electronic response is more appropriate and how responses will differ based on U.S. relations with the countries that originate the attack.
http://www.military.com/news/article/computer-hack-risks-cyber-jdam-strike.html

New crypto virus a looming threat

BY: ELLEN MESSMER, NETWORK WORLD
06/05/2008

A new variant on a virus is capable of encrypting a victims' data with an algorithm so strong that the encryption has defied all efforts to crack it so far. Criminals leave a text file for victims that offer to sell them a decryptor. Roel Schouwenberg, senior antivirus researcher at Kaspersky Lab explains that a similar virus spread about a year and a half ago, but that the encryption was much weaker, and easier to crack. Kaspersky labs recommend backing up data vigorously due to the new virus threat. Kaspersky Labs also recommends that victims do not give in to criminal blackmail and buy the decryptors to weaken the virus' impact.
http://www.networkworld.com/news/2008/060508-crypto-virus.html

NIST seeks comments on scheme to score IT security configurations

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
06/05/2008

The draft of the "Interagency Report 7502: The Common Configuration Scoring System" has been released for public comment from the National Institute of Standards and Technology. The draft is part of an effort to develop a standardized system to evaluate the impact of security configurations on operating systems. The report proposes a set of measures and formulas to "score" security configuration issues.

http://www.gcn.com/online/vol1_no1/46398-1.html

Air Force calls for help in building cyberwarfare skills

BY: WILLIAM MATTHEWS, THE FEDERAL TIMES
06/04/2008

The Air Force has published a request for white papers that will help the service achieve Dominant Cyber Offensive Engagement. The Air Force Research Laboratory is planning a budget of $3 million in 2008 and $8 million in 2009 to develop new cyberwarfare technologies. The Air Force wants to develop cyberwarfare skills including taking full control of a network, gaining access to remote or closed computer systems, gaining access to "any and all operating systems", maintaining a presence in adversary information infrastructure, and disrupting and destroying a computer system.
http://www.federaltimes.com/index.php?S=3562360

Cyberspace becoming more malicious

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
06/04/2008

Mark Sunner, MessageLabs' chief security analyst explains that the number of spam and malware email messages are increasing, and are become extremely common in public and manufacturing sectors. He also states that the government is a primary target for malware, due to the amount of vulnerable sensitive information in electronic databases. There has also been an increase in phishing and identity theft online. Sunner states that there are more security programs being built into the internet, but that new security programs must keep up with increasing malicious traffic.
http://www.gcn.com/online/vol1_no1/46393-1.html

Air Force talks about missions in cyberspace

BY: MICHAEL GILBERT, THE NEWS TRIBUNE
06/04/2008

Col. Tony Buntyn emphasized the importance of integrating cyberspace into United States military war-fighting doctrine in a presentation at the Pacific Northwest National Security Forum. Buntyn explained how the $5 billion a year command will be spread out among bases, and states that creating a cyberspace command is "a strategic imperative" for the Air Force. Buntyn explains that some U.S. adversaries already use the internet and the full electromagnetic spectrum to command and control, and have an understanding of cyberspace that the United States does not yet have.
http://www.thenewstribune.com/news/military/story/380091.html

Intelligence community seeks to go virtual

BY: WADE-HAHN CHAN, FEDERAL COMPUTER WEEK
06/03/2008

Assistant deputy director and chief technology officer Michael Wertheimer predicts that the next frontier in battling espionage will be in the virtual world. Intelligence community officials have put together a four week summer exercise, called the Summer Hard Problem Program, to learn more about cyber space and the technologies available to cyber criminals.
http://www.fcw.com/online/news/152713-1.html

Malicious software threatens internet economy

BY: COLIN BARRAS & TOM SIMONITE, NEWSCIENTIST.COM
06/02/2008

A report from the Organization for Economic Co-operation and Development (OECD) states that national economy and security faces a growing threat from malicious software. Malware is most commonly used to turn an ordinary PC into a "zombie" computer, which can be controlled by criminals without the knowledge of the owners. The OECD states that international cooperation and agreements are needed to analyze malware attacks and develop a system to counteract them. The full OECD report *Malware: A security threat to the Internet Economy* is available to download through the article.
http://technology.newscientist.com/channel/tech/dn14034-malicious-software-threatens-internet-economy.html

Chinese hackers pose serious danger to U.S. computer networks

BY: SHANE HARRIS, NATIONAL JOURNAL
05/29/2008

According to U.S. government officials and computer security experts, computer hackers in China, including some working on behalf of the Chinese government, have penetrated information systems of U.S. companies, stolen information and gained access to electric power plants in the United States. Chinese hackers have been blamed for two blackouts from attacking electric power plants, and have also been accused of accessing business information before negotiation meetings between Chinese and United States businesses. China has been identified as a primary threat to U.S. cyber security and the Defense Department has warned that China is "building capabilities for information warfare" for possible use in "pre-emptive attacks."
http://www.govexec.com/dailyfed/0508/053008nj1.htm

Cyber criminals overseas steal U.S. electronic health records

BY: BOB BREWIN, NEXTGOV
05/16/2008

United States electronic health records were stolen and found on a computer server in Malaysia, which is controlled by cyber criminals. Criminals can create false billing, which can bring in millions of dollars from stolen health records. The discovery of the stolen records has revealed the vulnerability of electronic medical records, and can cause more damage than the loss of money to false billing. If cyber criminals alter a patient's medical records, the results could be potentially deadly.
http://www.nextgov.com/nextgov/ng_20080516_2203.php

Comcast Is Hiring an Internet Snoop for the Feds

BY: NOAH SHACHTMAN, WIRED BLOG NETWORK
05/30/2008

Comcast, the nation's second largest internet provider, is looking for an engineer to analyze subscriber intelligence as part of the company's National Security Operations. Job duties would include installing/removing data intercept equipment to met Government standards as well as processing traffic on the company's digital voice and high speed internet services. Applicants

must also be knowledgeable with Communications Assistance for Law Enforcement Act (CALEA).
http://blog.wired.com/defense/2008/05/comcast-wants-d.html

Expert dissects Estonian cyber-war

BY: SHAUN NICHOLS, PERSONAL COMPUTER WORLD
05/22/2008
Gadi Evron, a security researcher shares his account of the cyber attacks on Estonia, and is offering advice to prevent similar attacks. Evron's article, which was published in the Georgetown Journal of International Affairs, explains that the internet attacks began in April as part of an outbreak of riots and cyber attacks from Russians living in Estonia, in response to the transfer of a Russian WWII memorial. Evron emphasizes that there was no clear leadership for responding to the attacks, and encourages all governments to develop a clear response plan.
http://www.pcw.co.uk/vnunet/news/2217276/expert-reflects-cyber-war

Crimeware defense strategies: how to protect your network (and yourself)

BY: JULIE BORT, NETWORK WORLD
05/29/2008
Markus Jacobson and Zulfikar Ramzan are co-authors of the new book, Crimeware: understanding new attacks and defenses, and participated in a live Network World Chat. They discuss rising trends in cybercrime, how hackers can make scams seem more genuine and new types of cyber attacks. They also give advice on warning signs of scams, such as email viruses, and how to defend your computer against an attack.
http://www.networkworld.com/chat/archive/2008/052908-crimeware-chat.html

U.S., China largest sources of Internet attacks

BY: JIM DUFFY, NETWORK WORLD
05/29/2008
Akamai Technologies, which operates a global server network, identified the United States and China as the two largest sources of cyber attacks during the first quarter of 2008. China and the U.S. accounted for 30% of all attack traffic. The first quarter report is available for download in the article, and the second quarterly report will be released in August.
http://www.networkworld.com/news/2008/052908-akamai-stateoftheinternet-report.html

Comcast.net Hijacked, Redirected

BY: DAVID KRAVETS, WIRED BLOG NETWORK
05/29/2008
During an overnight attack on Comcast.net, the Comcast homepage was redirected to a page boasting of the hack. A spokesperson for Comcast said that there was no evidence of trapping passwords or intercepting email, although the hackers certainly had access to the email accounts, and that the attack was only defacement. The hackers acquired the domain management account login information from Network Solutions, and the registrar is still conducting investigations as to how the login information was released.
http://blog.wired.com/27bstroke6/2008/05/comcast-servers.html

Comcast Hijackers Say They Warned the Company First

BY: KEVIN POULSEN, WIRED BLOG NETWORK
05/29/2008

The two hackers responsible for taking down Comcast's homepage and webmail service overnight May 28, identified as Defiant and EBK, participated in an hour long phone conference with Threat Level. The hackers, who are members of the underground group Kryogeniks, expressed both jubilance and nervousness over the impact of their attacks. The hackers state that they warned Comcast of the attacks before they were launched, and that the attack was launched as a response to bad service from Comcast.
http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html

Comcast Site Is Briefly Hacked

THE WALL STREET JOURNAL
05/29/2008

Comcast Corp., which provides email, news and technical support to over 14 million subscribers, was hacked and defaced for several hours overnight on Wednesday May 28. The hackers seized control of the Comcast domain name and redirected it to other servers. Spokeswoman Jennifer Khoury said that the damage was reversed early Thursday, although some email accounts were still down, and that Comcast was working with law enforcement authorities.
http://online.wsj.com/article/SB121208034553129769.html

Wireless Opens Tactical Horizons

BY: HARRISON DONNELLY, MILITARY INFORMATION TECHNOLOGY
04/09/2008

Military specialists are experimenting with a range of methods for deploying large amounts of date wirelessly, in order to increase command and control communications capabilities for cyberwar. The Pentagon recently funded a $1.4 million "quick reaction" technology program, which will develop a prototype mobile ad hoc wireless network to deploy information wirelessly. Called "mesh networking", the prototype will route data, voice and instructions between nodes, make continuous connections and even reconfigure around broken or blocked paths.
http://www.military-information-technology.com/article.cfm?DocID=2397

Outside View: Cyber-war realities

BY: ILYA KRAMNIK, SPACE WAR
05/28/2008

Cyberspace is becoming an increasingly large part of our everyday lives, especially in the areas of modern warfare, military systems and the expansion of the war zone. To be successful in modern warfare, an army must have extremely large, yet vulnerable, computer information systems. There is also much debate about the impact of cyber warfare, and whether an attack on network security should be considered more or less dangerous than traditional war fighting methods.
http://www.spacewar.com/reports/Outside_View_Cyber-war_realities_999.html

EC launches IPv6 adoption initiative

BY: WILLIAM JACKSON, GOVERNMENT COMPUTER NEWS
05/28/2008

The European Commission announced a plan to adopt IPv6 networking, aiming to increase the number of industry, public authorities and households on IVp6 to 25% by 2010. IPv6 was created to address shortcomings in the current IPv4 system, including a limited number of available web addresses and less network security. Although the EC will introduce and promote the initiative, they will not issue a mandate requiring a switch to IPv6, like the United States government. Both Europe and the United States are making efforts to keep up with the rapid transfer to IPv6 in Asia.
http://www.gcn.com/online/vol1_no1/46359-1.html

Systems for Cyber Control

BY: ADAM BADDELEY, MILITARY INFORMATION TECHNOLOGY
06/01/2008

The Air Forces Cyber Control Systems (CCS) program is in the early stages of contract competition to provide command and control of systems, awareness of network activity and a response plan to developing cyber threats. The CCS program will focus on utilizing all available sources to gather information on cyber security, and will not act as an offensive system. The article also includes interviews with three companies that have expressed interest in the development of CCS.
http://www.military-information-technology.com/print_article.cfm?DocID=2398

Taking Command In Cyberspace

BY: JOHN RENDLEMAN, GOVERNMENT COMPUTER NEWS
05/27/2008

Lt. Gen. Michael Peterson, chief information officer at the Air Force, is taking the lead in connecting computer and network systems into a “unified global command-and-control platform known as Cyber Command.” Peterson states that there have been significant strides made in Cyber Command since its introduction in 2005; however, he also recognizes that cyber attacks are increasing in numbers and sophistication. Peterson also emphasizes the importance of utilizing service-oriented architecture, and sharing information while still protecting confidential systems.
http://www.gcn.com/print/27_12/46315-1.html

The Next Revolution in Productivity

BY: RIC MERRIFEILD, JACK CALHOUN, DENNIS STEVENS, HARVARD BUSINESS REVIEW
06/01/2008

Service-oriented architecture (SOA) is a relatively new way of designing and utilizing the software that controls business activities. SOA, much like the introduction of Six Sigma and other quality improvement tools, is increasing the efficiency of businesses, cutting down on costs and reducing repetitive nonessential tasks that could easily be outsourced or removed altogether. Many businesses are still using twentieth century operating models or think that SOA is too technical to implement, however the business leaders who do pioneer plug-and-play businesses would enjoy a great leap in productivity.

http://harvardbusinessonline.hbsp.harvard.edu/hbsp/hbr/articles/article.jsp?ml_action=get-article&articleID=R0806D&ml_issueid=BR0806&ml_subscriber=true&pageNumber=1&_requestid=44005

Next-Generation Online Cons

BY: CLAY SHIRKY, HARVARD BUSINESS REVIEW
06/01/2008

Online scams which are more efficient and profitable than face to face scams, are part of a rising trend of online crime. Criminals are able to set up long-term scans by making fake businesses, intercepting business or customer information, or hacking into a legitimate website. Online cons do not require a large amount of money, and can be performed by amateurs, making online cons even more dangerous to businesses and customers. Businesses should take measures to protect themselves from scams, including collaborating with other businesses and making sure that their customers can tell between their business and a fake.
http://www.harvardbusiness.com/hbsp/hbr/articles/article.jsp;jsessionid=LPDP4MEBQNK5OAKRGWDSELQBKE0YIISW?ml_action=get-article&articleID=F0806D&ml_issueid=BR0806&ml_subscriber=true&pageNumber=1&_requestid=15434

CYBER WAR! Frontline

PBS.ORG
PUBLISHED 04/24/2003

Former chairman of the White House Critical Infrastructure Protection Board explains the difference between traditional war fighting methods and advancing cyber war methods. The report examines how criminal groups, including Al Qaeda, have already penetrated United States critical infrastructure. The Frontline report emphasizes the dangers of cyberattacks, and the importance of getting ahead of the curve, to stop potential attacks rather than reacting to them.
http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/synopsis.html

CORRECTIONS / CLARIFICATIONS

The following corrections and/or clarifications to the previous edition of CyberPro are provided based on subscriber feedback.

NATO to set up cyber warfare center

BY: ROBERT MCMILLAN, PC WORLD
05/14/2008

The Estonian cyber defense Centre of Excellence is not "owned" by NATO. Rather, it is being sponsored by seven NATO nations and the Allied Command Transformation. For more information: http://www.nato.int/docu/update/2008/05-may/e0514a.html .

Analysis: USAF's cyber offense capability
OKIE CAMPAIGNS
05/17/2008

The NSCI summary mentioned the USAF's pursuit of an offensive cyber capability and a NATO-sponsored cyber defense center to be based in Estonia. This was not intended to imply NATO, or Estonia, are in anyway pursuing an offensive cyber capability through the newly established Centre of Excellence (COE).

CyberPro Content/Distribution

This newsletter is intended to serve as a snapshot of Cyber-related events and issues, and is distributed every two to three weeks. Feel free to forward this newsletter to other interested individuals. If you have information you think should be included, or if you would like to be added or removed from distribution, please e-mail Larry McKee.

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest. The views, opinions, and/or findings and recommendations contained in this summary are those of the original authors and should not be construed as an official position, policy, or decision of the United States Government, U.S. Department of Defense, or the National Security Cyberspace Institute.