CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and 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 are not intended 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/or possible administrative, civil, and/or criminal action.

The views, opinions, and/or findings and recommendations contained in this summary are those of the 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.

Please contact Larry McKee , ph. (757) 871-3578, regarding CyberPro subscription, sponsorship, and/or advertisement.

o

The Cyber Innovation Center (CIC), Eighth Air Force (8AF) and Air Force Cyber Command (AFCYBER) Provisional are co-sponsoring the 2008 Cyber Awareness Summit in Bossier City - Shreveport, Louisiana on October 7-9, 2008. Cyber touches almost every aspect of our daily lives as it encompasses physical, logical and social networks. This Summit explores the "connectedness" that is cyber and its transformative effect on critical infrastructure, business and society. The objectives of the Cyber Awareness Summit are simple, but bold:

- Raise awareness about cyber related opportunities and concerns;
- Explore cyber's transformative effect on society (business relationship and structures, social networking, workforce development, education, and social engineering);
- Examine the resulting interdependencies created across government, industry and academia; and,
- Provide a venue for social networking within the cyber community.

For more information visit www.cyberinnovationcenter.org

CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

TABLE OF CONTENTS

CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

CYBERSPACE BIG PICTURE

What are Cisco's top network-management challenges?

BY JIM DUFFY, NETWORK WORLD
09/03/2008

Cisco has had network management issues for years, partly due to their acquisition of 125 companies since 1993. Karen Sage, Cisco's director of product management for network management states that it is actually a good sign that network management is struggling because it is a mark of a high rate of innovation. Sage explains that the top needs of Cisco customers in the area of network management are service automation for deployment and tracking, specific metrics for specific domains, and the ability for Cisco applications to interact with customer's applications. Customers have also expressed the need for a better user interface for Cisco IOS software.
http://www.networkworld.com/news/2008/090308-cisco-network-management-challenges.html

Cyberwar fears grow after Georgia websites attacked

NEWSCIENTIST.COM
09/01/2008

The distributed denial of service (DDOS) attacks in Georgia are most likely the work of politically motivated hackers according to US analysts. The attacks have US officials concerned that these bands of independent "cyber militias", who have little or no connection to a particular state will now have more power and influence over international affairs through cyberattacks. The U.S. and other Western nations are concerned because so much of their infrastructure is linked to the internet including finance, commerce, air traffic, communications and power grids, which are all vulnerable to cyber attack.
http://technology.newscientist.com/channel/tech/dn14635-cyberwar-fears-grow-after-georgia-websites-attacked.html

U.S. to deploy DNS Security in two years

SECURITY FOCUS
08/28/2008

The United States government has issued a memo mandating that all major agencies adopt DNSSEC technology, which secures the domain name system (DNS) against attacks, by December 2009. The system requires public-key cryptography. Because of this, and other technical issues, the government and private sector companies have resisted implementing DNSSEC for more than a decade. DNS infrastructure experts have recommended implementing source-port randomization as a patch for the DNS security vulnerabilities, rather than adopting the technology as a solution to the attacks.
http://www.securityfocus.com/brief/807?ref=rss

Terror threat system crippled by technical flaws, says Congress

BY: PATRICK THIBODEAU, COMPUTER WORLD
08/27/2008

A staff memo from the Subcommittee on Investigations and Oversight states that a $500 million IT project designed to help prevent another 9/11 is a failure. A data integration project, called Railhead, was intended to help intelligence and law enforcement agencies uncover terrorist plots is suffering from delays and cost overruns and may need to close down completely. The subcommittee obtained user-group meeting minutes, e-mails, internal blog postings and technical reports that first raised issues about the project. The Railhead software, which was tested by the Hewlett-Packard

Quality Center, passed 148 tasks, did not complete 26, and failed 42.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113658&source=rss_topic17

Pentagon Worries About Chinese Chips

BY: ANDREW T. GILLIES, FORBES
09/04/2008

Ted J. Glum, director of the Department of Defense's Defense Microelectronics Activity unit spoke at the 2008 Common Defense Conference, and stated that 90% of the DoD's obsolescence problems are related to electronics. Glum explained that the military uses more microelectronics than ever, but that it purchases just 0.1% of the world's semiconductors. Quality is one issue the Department of Defense must address. The Department of Defense also predicts that most chip foundries by 2014 will be found in Asia, which is known for counterfeiting.
http://www.forbes.com/2008/09/04/pentagon-defense-contractors-biz-wash-cz_atg_0904beltway.html

The threat from within

BY: COL. PETER R. MARKSTEINER, ARMED FORCES JOURNAL
09/06/2008

Joint Publication 3-13, "Information Operations (IO)" states that anything that degrades or denies information is an IO threat, and cautions military leaders against evolving technologically based threats. Information overload is blamed for making commanders and decision-makers less aware and less capable of resolving complex issues in military operations. Information overload is also gaining prominence for causing problems with productivity, having economic impacts and affecting worker health and satisfaction. The article recommends streamlining e-mails, maintaining focus on missions and limiting information overload.
http://www.armedforcesjournal.com/2008/09/3640424

Pentagon debates development of offensive cyberspace capabilities

BY JULIAN E. BARNES, LOS ANGELES TIMES
SEPTEMBER 8, 2008

Senior military officials are encouraging the Pentagon to develop capabilities to attack other nation's computer systems rather than focusing on defending the United States' electronic security. U.S. officials have so far been reluctant to militarize the Internet, which they saw as a medium for commerce and communication. The new National Military Strategy for Cyberspace Operations which was declassified

earlier this year gave the military approval to begin developing expanded capabilities.
http://www.latimes.com/news/printedition/front/la-na-cyber8-2008sep08,0,909623.story

DOD wants contractors to focus on data security

WASHINGTON TECHNOLOGY
09/09/2008

Trey Hodgkins, vice president of federal programs for the Information Technology Association of America, explains that the Defense Department has been meeting with 25 systems integrators in an effort to secure government information. The Army also released a request for information in September. Vendors have until Oct. 6 to submit information on how they secure controlled unclassified information on their own systems to the Army's RFI. Hodgkins states that finding a solution by engaging industry is a step in the right direction for the Defense Department.
http://www.washingtontechnology.com/online/1_1/33478-1.html

Taking intelligence analysis to the virtual world

BY: BEN BAIN, FEDERAL COMPUTER WEEK
09/04/2008

Online virtual worlds are increasingly being seen as valuable tools for intelligence analysis. The Office of the Director of National Intelligence's Intelligence Advanced Research Projects Activity program is designing a project that will examine how virtual worlds can be used for analyst training. The project, A-SpaceX, will examine how to use and develop virtual worlds to use time frame manipulation and mapping decision processes for improving intelligence analysis. Other projects include the Knowledge Discovery and Dissemination project which will explore how information technology can better handle the large amount of information that analysts receive.
http://www.fcw.com/online/news/153689-1.html

Widespread cell phone location snooping by NSA?

BY: CHRIS SOGHOIAN, CNET
09/08/2008

A recent article in the London Review of Books reported that the majority of the National Security Agency's warrantless wiretapping is occurring under the radar, rather than with major wireless companies like AT&T, Verizon and Sprint. Many small companies have small roles in the wireless phone industry, but are able to learn a lot about the calling habits of Americans. Also, laws regarding information sharing and wiretapping apply specifically to companies that provide services to the general public, but do not cover firms that provide services to those major carriers. Because of this, the NSA can go to firms that own and operate wireless towers for large carriers for information, while avoiding gathering information from the major carriers themselves.
http://news.cnet.com/8301-13739_3-10030134-46.html?tag=newsLatestHeadlinesArea.0

Remember to Look Next to You When Eliminating IA Threats

SIGNAL
08/2008

The Army's defenses against cyber attacks are state of the art and include the best available tools such as firewalls and virus scanners, but a large percent of malicious network attacks come from inside the organization. Internal threats usually come from disgruntled employees, or sometimes accidentally by untrained employees. This article provides some suggestions for improving protection against internal threats including establishing out-processing policies, deleting accounts of past employees, maintaining internal forensic

tracking tools, fully training all employees and inspects and auditing computers periodically. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1684&zoneid=238

Navy details NMCI follow-on plan

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
09/05/2008

Documents release by the Navy outline plans for the future of the Navy Marine Corps Intranet (NMCI), including changing the Intranet's name to Next Generation Enterprise Network. According to Pat Tracey, an EDS vice president and retired Naval Admiral, explained that the Intranet will be integrated more tightly on some networks, such as the networks ships use at sea, although ashore environments would be integrated as well. EDS is the prime contractor on the 10-year NMCI project. http://www.fcw.com/online/news/153710-1.html

DISA's NECC forges joint command and control with SOA

BY: BRIAN ROBINSON, DEFENSE SYSTEMS
09/08/2008

The Department of Defense is modernizing its command and control (C2) infrastructure with the hopes of reducing costs of developing C2 capabilities, and developing a faster way to deliver new capabilities to warfighters. The new C2 environment, called the Net-Enabled Command Capability will be released in fiscal 2010 as an initial operational version, followed by a complete operational version in fiscal 2011. Lee Whitt of Northrop Grumman Mission Systems states that there will be issues because no one is sure how to test and evaluate SOA-based systems, and even if the service is compliant with Web standards, it must be practical and efficient for warfighters to use. Warren Suss, president of Suss consulting, has followed the DoD's strategy for SOA-based C2 from the beginning and states that there is a lot of standards identification and compatibility issues that must be addressed. http://www.defensesystems.com/issues/3_7/features/1804-1.html#

ISO slated over Microsoft cave-in

BY: ELIZABETH MONTALBANO, IDG NEWS SERVICE
09/03/2008

Brazil, South Africa and Venezuela said that they are "no longer confident" in the ability of the International Organisation for Standardisation and the International Electrotechnical Commission to be vendor neutral when it comes to technology standards in a statement at the Congresso Internacional Sociedade e Governo Electronico 2008 conference. The countries had protested the decision to approve Microsoft's OOXML as an international standard. The appeals were dismissed, and the three countries will not pursue their appeals. http://www.techworld.com/news/index.cfm?RSS&NewsID=103855

CYBERSPACE RESEARCH

New Metrics Assign Grades to Your Security Posture

BY: KELLY JACKSON HIGGINS, DARK READING
09/08/2008

The nonprofit Center for Internet Security hopes that a set of metrics released by a coalition of government agencies, universities and vendors will serve as a standard for assessing network security. The metrics will provide a number grade which will help companies evaluate their security and determine better security buying decisions or strategies. The first set of metrics that CIS will release will include time between security

incidents, recovery time from incidents, percentage of systems that are configured correctly, percentage that are patched appropriately, percentage of systems with anti-virus software and percentage of business applications that have had a penetration or security assessment.
http://www.darkreading.com/document.asp?doc_id=163211

Army seeks information assurance ideas

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
09/01/2008

The Army issued a request for information about information assurance programs; specifically, Army officials are researching how contractors identify digital data and protect it from unauthorized access and release as well as how they handle encrypted data. David Wilson, vice president of product management and support at Telos explains that the request for information is an acknowledgement of current vulnerabilities and flaws in information assurance. The request was issued by the Program Executive Office for Enterprise Information Systems and the Assistant Secretary of the Army for Acquisition, Logistics and Technology.
http://www.fcw.com/online/news/153662-1.html

Report: Popular Web Attacks Go Stealth

BY: KELLY JACKSON HIGGINS, DARK READING
08/27/2008

A report released recently by WhiteHat Security found that the most popular online attacks were encoded SQL injection and cross-site scripting (XSS) attacks, which are harder to catch than the previous SQL and XSS attacks which were not encoded. ScanSafe has reported that there was an 87% jump in malware from June to July this year, 75% of which is attributed to the new SQL injection attacks. The WhiteHat report also lists Internet security vulnerabilities according to how likely they are to be on a website. XSS attacks are number one on the list and information leakage, content spoofing, insufficient authorization and SQL injection are also all in the top ten.
http://www.darkreading.com/document.asp?doc_id=162515&f_src=darkreading_section_296

Revealed: The Internet's Biggest Security Hole

BY: KIM ZETTER, WIRED BLOG NETWORK
08/26/2008

Two security researchers demonstrated an Internet security vulnerability which could be larger and more dangerous than the vulnerability found in the DNS System. The vulnerability uses the Internet's Border Gateway Protocol (BGP) which allows a hacker to monitor internet traffic worldwide and change information before it reaches its destination. This vulnerability has been a theoretical security issue since it was first addressed in 1998, but some argue that this protocol is different because hackers would not be exploiting a weakness in the protocol, but would be exploiting the natural way that BGP works. Anton "Tony" Kapela, network director at 5Nines Data, and Alex Pilosov, CEO of

Pilosoft, demonstrated how to exploit the vulnerability at the DefCon hacker conference in Las Vegas.
http://blog.wired.com/27bstroke6/2008/08/revealed-the-in.html

Report: Botnets quadruple

BY: KATHLEEN HICKEY, GOVERNMENT COMPUTER NEWS
09/08/2008

According to the Shadowserver Foundation, the number of botnet infected computers has jumped from 100,000 to 400,000 PCs over the past three months. Botnets are networks of infected machines which are controlled by a single machine and participate in spam and phishing attacks. The jump in infected machines is attributed to an increase in SQL injection attacks and groups are getting better at hiding their bots. Botnet communication also looks much like normal Internet traffic and tends to pass through firewalls easily.
http://www.gcn.com/online/vol1_no1/47092-1.html

CYBERSPACE EDUCATION & TRAINING

Cybersecurity Site Launches for Non-Techies

DARK READING
09/10/2008

The Internet Protectors website offers a neutral environment for computer users to find non-technical help in learning about protecting themselves and their computer networks. The site allows users to ask questions of security experts, read blogs on security topics, discuss issues in forums and research security through podcasts and whitepapers. Pat Bitton, co-founder of The Internet Protectors, explains that there is currently no place for everyday computer users to find information about protecting themselves online.
http://www.darkreading.com/document.asp?doc_id=163402&WT.svl=wire_3

Air Force to restructure IT career paths

BY: KEVIN FOGARTY. DEFENSE SYSTEMS
09/02/2008

Maj. Gen. John Maluda, director of cyberspace transformation and strategy and secretary of the Air Force's Office of Warfighting Integration and chief information officer announced that the Air Force's IT ranks will reduce by 8200. The Air Force intended to make up for the reduction by increasing the efficiency of its technology, but there may be a significant shift in the career paths of technical specialists. The Air Force will increase the number of specialists who can participate in cyberwarfare instead of focusing on securing information and networks of individual bases, and will also rely more heavily on civilian and industry resources.
http://www.defensesystems.com/cgi-bin/udt/im.display.printable?client_id=defsysmag_news&story_id=1793

Air Force IT Conference highlights education

BY: SCOTT KNUTESON, AIR UNIVERSITY PUBLIC AFFAIRS
09/02/2008

The Air Force announced the "AF.EDU" project at the Air Force Information Technology Conference on August 26. The project aims to provide education and training for Airmen and Air Force civilians through collaboration throughout the Air Force and worldwide colleagues. The program will use simulation in cooperation with NATO to train Airmen in emergency response. The AF.EDU site, which currently requires authentication through an account, will soon feature "AF.EDU Public" where information will be available publicly,

and "Keesler Online" which will be available to all Air Force users.

http://www.af.mil/news/story.asp?id=123113256

GEORGIA CYBERATTACK

Botnets Behind Georgian Attacks Offer Clues

BY: KELLY JACKSON HIGGINS, DARK READING
09/09/2008

Arbor Networks researchers Danny McPherson and Jose Nazario released new findings about botnets behind the cyber-attacks on Georgia at the closed-door Internet security summit in Estonia this week. Their research found that Georgia launched distributed denial-of-service (DDOS) attacks against Russia, and found no evidence that either Russia or Georgia's attacks were completely state-sponsored. Surprisingly, they also found that both Russian and Georgian sites were both being attacked by third party botnets. The command and control of one of these botnets is located in the United States.
http://www.darkreading.com/document.asp?doc_id=163342

Cybervasion as viruses attack national websites

BY: SHAUN WATERMAN, GEELONG ADVERTISER
08/28/2008

The cyber attacks on Georgia were monitored by sever US Internet watch operations, including US-CERT, who did not participate in a response but did pass on information about the Distributed Denial of Service attack to DHS intelligence analysts. DDOS attacks bombard servers with messages and requests from a network of computers under the control of hackers, which can cause the victim servers to crash. Steven Adair of ShadowServer states that the registration information of the internet domain that originated the attacks gives a Russian contact address, but some believe the real attackers are trying to pin the blame on Russia.
http://www.geelongadvertiser.com.au/article/2008/08/28/17725_opinion.html

CYBERSPACE COMMAND

BLOG: Air Force Cyber Command could return, with nukes

BY: NOAH SHACHTMAN, WIRED
09/09/2008

The Air Force's Cyber Command, which has been put on hold, may be coming back with focus on nuclear capabilities as well as cyber. Air Force nuclear and cyber troops may be combined into a "Global Effects Command" which would work with U.S. Strategic Command. Many speculate that this would be similar to the previous Strategic Air Command, but would include protection for cyberspace as well as "deter foes with missiles, bombers, or electrons."

http://blog.wired.com/defense/2008/09/afcyber-ii.html

Cyber efforts get official support

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES
09/03/2008

A summit was recently called to discuss the future of the Air Force Cyber Command and included Air Force Chief of Staff Gen. Norton A. Schwartz, Chief Master Sgt. of the Air Force Rodney J. McKinley and other secretaries, command heads and Headquarters Air Force staffers. A release following the conference states that the establishment of the Command should continue and that the mission of the Air Force includes fighting and winning in

cyberspace as well as air and space. Progress reports were also presented on other agenda items including Unmanned Aircraft Systems manning initiatives, personnel end strength and Common Battlefield Airman Training.
http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=2008809030377

Cyber troopers gearing up to go for the Gustav

BY: JOHN ANDREW PRIME, SHREVEPORT TIMES
09/05/2008

The Cyber Command has organized the Air National Guard information technology specialists to be prepared to help storm-battered south Louisiana. A dozen senior enlisted or veteran sergeant specialists have been armed with gear including generators, transmitters, computers and portable radio towers to help restore computer networks, the Internet and cellular communications to aid recovery and providers.
http://www.shreveporttimes.com/apps/pbcs.dll/article?AID=/20080905/NEWS01/809050340/1060

New leader at cyber command departs

BY: DOUG BEIZER, FEDERAL COMPUTER WEEK
08/29/2008

Maj. Gen. Randal Fullhart will leave his position as vice commander of the provisional Air Force Cyberspace Command to a new position as director of Global Reach Programs in the Office of the Assistant Secretary of the Air Force for Acquisition at the Pentagon. Leaders are considering delaying setting up the Air Force Cyberspace Command, but Fullhart states this his move should not be taken as an indication that any decision has been made.
http://www.fcw.com/online/news/153656-1.html

CYBERSPACE HACKS, TACTICS AND DEFENSE

Gas refineries at Defcon 1 as SCADA exploit goes wild

BY: DAN GOODIN, THE REGISTER
09/08/2008

Exploit code that was published as a module to the Metasploit penetration testing toolkit attacks a vulnerability in CitectSCADA, which makes gasoline refineries, manufacturing plants and critical facilities vulnerable to attacks. Kevin Finisterre, the director of penetration testing at Netragard and the creator of the exploit claims most users that received a security advisory will not take immediate action. There is much confusion surrounding the disclosure of the security flaw because theoretically the flaw is not very dangerous to organizations who take proper precautions, as their critical industrial controls should not be exposed to the Internet.
http://www.theregister.co.uk/2008/09/08/scada_exploit_released/

Hack Lets Researchers Silently Eavesdrop on IP Networks

BY: TIM WILSON, DARK READING
08/27/2008

Researchers Anton "Tony" Kapela and Alex Pilosov demonstrated how to exploit a vulnerability in the Border Gateway Protocol (BGP) at the Defcon hacker conference in Las Vegas. The vulnerability would allow hackers to intercept Internet traffic without the sender or receiver knowing that the information had been intercepted. The researchers explain that only analysis of BGP routing tables and filtering could detect the hack, but both detection and filtering are complex processes and are not currently used.
http://www.darkreading.com/document.asp?doc_id=162491

CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

The Spawn of Storm Rides Again

STRATEGY PAGE
08/27/2008

Despite the publicity of the Storm virus, hackers are continuing to spread the virus through email by simply changing the subject of the infected emails. Emails that claim to have news information about the conflict in Georgia or the Olympics ask the user to open a .zip or .pdf file which will infect the user's computer with a Trojan horse virus. The Storm virus turns victim computers into "zombies" which help to spread the virus or participate in DDOS attacks. The source of the virus has still not been identified although the virus can be traced to Russia. The Russian government refuses to cooperate with investigations, and the investigation also indicates that some of those responsible may be American.
http://www.strategypage.com/htmw/htiw/articles/20080827.aspx

The Lights Are Going Out All Over Europe

STRATEGY PAGE
08/30/2008

European nations are alarmed over an increase of Internet probes of public utilities. Criminals can find information on how to shut down utilities, and then extort money by threatening to shut them down, or damage utilities as part of a military operation. The probes can be traced to China, Eastern Europe and the Middle East. Although there have been no known attacks so far, utilities and other large corporations are urged to check the adequacy of their security defenses.
http://www.strategypage.com/htmw/htiw/articles/20080830.aspx

Microsoft patches will put IT on hunt for affected systems

BY: JOHN FONTANA, NETWORK WORLD
09/09/2008

Microsoft released four critical patches which target vulnerabilities in Windows-based server and client operating systems, the worst of which was the MS08-052, which addresses five vulnerabilities and affects the core operating system. According to Amol Sarwate, manager of the vulnerabilities research lab at Qualys, the vulnerability affects .bmp, .wmf, and .gif file formats that could easily be transmitted by e-mail or viewing malicious websites. MS08-052 affects versions of Internet Explorer, Windows XP and Vista, Windows Server, Office XP 2003 and 2007, Visio, Visual Studio and other Microsoft software.
http://www.networkworld.com/news/2008/090908-microsoft-patches.html

Zombie plague sweeps the internet

BBC NEWS
09/04/2008

The Shadowserver Foundation reported that there has been at least a threefold increase in zombies in the last three months, and stated that more than 450,000 computers are now part of zombie networks run by hi-tech criminals. Zombie computers are used to send spam or junk mail, and can be used to launch attacks on websites, store stolen information, or participate in phishing scams. The Shadowserver Foundation believes that the jump in zombie computers is due to a series of attacks that infect malicious code on to legitimate websites.
http://news.bbc.co.uk/2/hi/technology/7596676.stm

CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

Microsoft tackles remote code execution with updates

BY: GRANT GROSS, TECHWORLD
09/05/2008

Microsoft releases security patches on Patch Tuesday, which is the second Tuesday of every month. Most recently, Microsoft released four patches which included fixes for a vulnerability that allows remote code execution in Windows Media Player 11, various versions of the Windows OS, Windows Media Encoder 0 and in Office and Office OneNote 2007. Microsoft released 12 updates in August including 7 that were critical, five critical patches in July, and two in June.
http://www.techworld.com/news/index.cfm?RSS&NewsID=103984

Report: N. Korea Used Spyware, Sex in Targeted Attack on S. Korean Military

DARK READING
09/03/2008

A military officer in charge of South Korea's military command and control system was the victim of a spyware attack from a North Korean email message. The attack automatically steals files from the victim's computer when the email is opened. A woman from South Korea was also arrested for giving a North Korean official name cards and emails of 100 South Korean military officers, and reportedly attempting to seduce military officers to gather information. Graham Cluley, a senior technology consultant wrote in his blog that many nations use the Internet and spyware for espionage and spying.
http://www.darkreading.com/document.asp?doc_id=162898&WT.svl=news1_1

At the Front Lines of Protecting the Internet

BY ROGER A. GRIMES, INFOWORLD
09/02/2008

VeriSign is well known for handling key DNS root servers and name resolution for .com, .net, and other domains. VeriSign has made PKI, SSL, TLS, EV and digital certificate security approaches commonplace, and spent millions of dollars building and protecting the Internet's massive DNS infrastructure. VeriSign has also angered some by adding new services to the

Internet such as domain waitlisting and higher registration fees. In this article, InfoWorld interviewed CTO Ken Silva, who manages VeriSign's technical operations.
http://www.pcworld.com/businesscenter/article/150572/at_the_front_lines_of_protecting_the_internet.html

Battling Botnets

BY: PETER A. BUXBAUM, MILITARY INFORMATION TECHNOLOGY
08/20/2008

Botnets were used last year in the distributed denial of service (DDOS) attack that was launched against computer networks in Estonia. The United States military has recently begun developing its own offensive and defensive botnet capabilities, partly in response to the attacks in Estonia. In the Armed Forces Journal, Air Force Col Charles Williamson advocated the development of botnet capabilities, and stated that the Air Force could use excess and obsolete computer capacity. The Air Force Research Laboratory (AFRL) posted a broad agency announcement stating that they wanted to develop botnet technology that would be capable of infiltrating offending systems, gathering information undetected and destroying enemy systems.
http://www.mit-kmi.com/article.cfm?DocID=2569

Mass. transit authority flaw disclosure: A student speaks up

BY: BILL BRENNER, COMPUTERWORLD
09/03/2008

Zack Anderson was one of the MIT students who found security flaws in the Massachusetts transit authority's fare system. The students planned to disclose their findings at the Defcon hacker conference in August, but were stopped by a gag order after the MBTA brought a lawsuit against the students. In this article, Anderson participates in an interview about the findings and the students' plans to sit down with the MBTA to discuss the security flaw and possible solutions.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114044

Evil Bits

BY: JOHN H. SAWYER, DARK READING
09/05/2008

There has been much press coverage lately about the WHH Ranch Company using shredded checks as packing material for twenty years without a single complaint. This article warns that hackers know the value in "dumpster diving" for bits of information that may be valuable. Employees discard notes with important information, and hackers can use these bits including passwords, IPs, and account numbers to gain access to internal networks. The article recommends that companies learn more about dumpster diving as part of their penetration testing to improve network security.
http://www.darkreading.com/blog.asp?blog_sectionid=447

Infamous Phishing Gang Joins Stealthy Botnet

BY: KELLY JACKSON HIGGINS, DARK READING
09/05/2008

Researchers from the RSA's FraudAction Research Lab believes the Rock Phish gang is moving operations to the more sophisticated Asprox botnet, which is known for large scale SQL injection attacks. Experts expect the gang to now be able to launch more Trojan attacks to steal more information and better evade detection. Researchers have determined that Rock Phish is using a command and control server on the Asprox botnet. The Rock Phish gang is based in Eastern Europe, and is responsible for over half of all phishing attacks worldwide.

http://www.darkreading.com/document.asp?doc_id=163045

Is Rock Phish cybergang set for a comeback?

BY: ELLEN MESSMER, COMPUTER WORLD
09/05/2008

The Rock Phish gang is an East European cybercrime group that creates botnets which they use in phishing attacks to steal personal information. The Rock Phish group developed the Zeus Trojan and is linking its Command & Control server with the Asprox botnet, which is a more advanced network for phishing attacks. The Asprox botnet has been linked to a massive surge of SQL-injection attacks earlier this year. According to RSA, the security division of the EMC Corporation, a drop in phishing attacks between June and August this year is partly due to the Rock Phish gang changing their attacks to the more powerful botnet.
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114168

Computer threat for industrial systems now more serious

BY: ROBERT MCMILLAN, NETWORK WORLD
09/10/2008

Kevin Finisterre published software last Friday that could be used to control computers that manage industrial machinery, which could let hackers into utility companies, water plants and oil and gas refineries. Finisterre, who is head of research with Netragard, states he aims to raise awareness of the vulnerabilities, and released the code as a software module for Metasploit. The code exploits a flaw in Citect's CitectSCADA software, which has a patch that has already been released. Citect has said that the flaw is only a security risk for companies who connect to the Internet without firewall protection. Citect is also planning to release a new version of CitectSCADA soon which will include new and improved security features.
http://www.networkworld.com/news/2008/091008-computer-threat-for-industrial-systems.html

CIA, FBI push 'Facebook for spies'

BY LARRY SHAUGHNESSY, CNN
09/05/2008

A new social networking site designed for spying organizations is increasingly being used by the CIA, the FBI and the National Security Agency. The program, called A-space is a networking site exclusively for analysts within the 16 U.S. intelligence agencies. Analysts could use the site to share information and opinion. The program has been in testing and officially launches on September 22. The material on A-Space would obviously be classified and would require an appropriate security clearance to access.
http://www.cnn.com/2008/TECH/ptech/09/05/facebook.spies/

CYBERSPACE – LEGAL

Employee has no privacy on company computers, US court rules

THE REGISTER
09/05/2008

A New Jersey court said that files on a work-owned computer can be searched with the company's permission, even if there is not consent from the computer user after a man was convicted of stealing $650,000 from his Certified Data Products while working as a bookkeeper. The man, referred to as MA, argued that his conviction was unsound because of the way the evidence was gathered. His laptop and desktop computers were searched without a warrant. The court stated that employees do have a right to use

employer's facilities with a reasonable amount of privacy, but employer's usage policies must be adhered to.
http://www.theregister.co.uk/2008/09/05/outlaw_us_privacy/

The Cyber Crime Hall of Fame

BY: CORINNE IOZZIO, PC MAGAZINE
09/08/2008

PC Magazine composed a list of nine cyber criminals that they found to be significant based on criteria such as ingenuity, the size of the crime, the cost of the damage and historical significance. Hackers include: John Draper, who was one of the first "hackers"; Kevin Mitnick, who gained access to all of the Pentagon and Department of Defense's files; and Gary McKinnon, who gained access to Air Force, Army, Navy, NASA, Pentagon and Department of Defense computers to find evidence of flying saucers. The article also ranks each hacker based on each criteria.
http://www.pcmag.com/article2/0,2704,2329604,00.asp

Infamous Israeli hacker linked to $1.8M heist

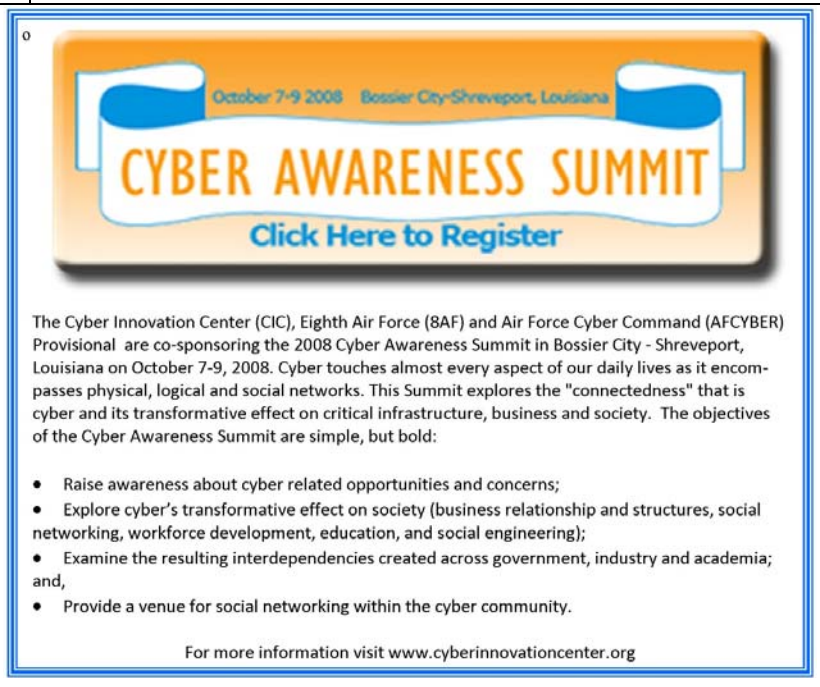
THE WINDSOR STAR
09/05/2008

Investigators spent nine months finding four suspects who stole $1.8 million from a Calgary company. The suspects are charged with stealing credit card information and fraud. One of the suspects, Ehud Tenenbaum, also accessed Pentagon computers. Tenenbaum has worked with Israeli organizations since his conviction to help the organizations protect their computer networks against attacks.
http://www.canada.com/windsorstar/news/business/story.html?id=df98c776-bbb9-4987-8526-6649e56c0574

CYBERSPACE-RELATED CONFERENCES

Note: Dates and events change often. Please visit web site for details. Please provide additions, updates, and/or suggestions for the CYBER calendar of events here.

15-17 Sept 2008	**24th Annual Air & Space Conference and Technology Exposition**, Washington D.C., http://www.afa.org
15-19 Sept 2008	**Interop New York,** New York, NY, http://www.interop.com/newyork/
18-19 Sept 2008	**Current and Future Military Data Links**, Washington D.C., http://www.asdevents..com/event.asp?ID=257
22 Sept 2008	**Net-Centric Operations Conference,** New Castle, N.H., http://herbb.hanscom.af.mil
25-26 Sept 2008	**Electronic Warfare Operations and Systems 2008**, London UK, http://www.asdevents.com/event.asp?ID=241
29-30 Sept 2008	**Airbone Networks Conference,** Washington D.C., http://www.asdevents.com/event.asp?ID=267
30 Sept – 2 Oct 2008	**National Security 2008**, Brussels, Belgium, http://www.asdevents.com/event.asp?ID=265
6-8 Oct 2008	**Strategic Space & Defense**, Qwest Center Omaha Convention Center and Arena, Omaha, NE, http://www.stratspace.org/
7-9 Oct 2008	**2008 Cyber Awareness Summit**, Bossier City-Shreveport, LA, http://www.cyberinnovationcenter.org/
16-17 Oct 2008	**8th Annual C4ISR Integration Conference** , Defense News Media Group, Arlington, Virginia, http://www.dnmgconferences.com/07c4isr/index.php?content=home
16-17 Oct 2008	**Cyber Security Conference,** Caesars Palace Hotel and Casino, Las Vegas, NV, **http://www.asdevents.com/event.asp?ID=319**
3-5 Nov 2008	**Global MilSatCom 2008 Conference & Exhibition,** Millennium Conference Centre, London, UK, www.smi-online.co.uk/08globalmilsatcom20.asp



CyberPro

Volume 1, Edition 9
September 11, 2008

Keeping Cyberspace Professionals Informed

CYBERPRO CONTENT / DISTRIBUTION

The articles and information appearing herein are intended for educational purposes to promote discussion in the public interest and 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 are not intended 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/or possible administrative, civil, and/or criminal action.

The views, opinions, and/or findings and recommendations contained in this summary are those of the 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.

Please contact Larry McKee , ph. (757) 871-3578, regarding CyberPro subscription, sponsorship, and/or advertisement.