Description of document:	US Department of Justice (DOJ) Justice Security Operations Center (JSOC) "News You Can Use" Newsletters, 2008-2011
Requested date:	11-April-2011
Released date:	20-May-2011
Posted date:	11-July-2011
Date/date range of documents:	Included are: Dec 2008, Feb-Sep & Nov 2009, Jan-Dec 2010, Jan-Apr 2011
Source of document:	FOIA Contact Justice Management Division Department of Justice Room 1111 RFK, 950 Pennsylvania Avenue, NW Washington, DC 20530-0001 Fax: 202-616-6695 Email: JMDFOIA@usdoj.gov

[redacted]

U.S. Department of Justice

Justice Management Division

Washington, D.C. 20530

MAY 20 2011

Re: Freedom of Information Act Request No. 23524997

I am responding on behalf of the Justice Management Division (JMD) to your Freedom of Information Act (FOIA) request dated April 11, 2011, for copies of each News You Can Use newsletter published on DOJNet. Because I deem you to be a non-commercial requester, you are entitled to the first 100 pages of documents and the first two hours of search time at no charge. 28 C.F.R. § 16.11(d).

I am enclosing, at no cost to you, all the News You Can Use newsletters that have been published on DOJNet, a total of 26 documents. We are withholding portions of four newsletters -- those from September 2010, August 2010, January 2010, and April 2010 -- under FOIA Exemption 7(E), which protects disclosure of law enforcement techniques and procedures. 5 U.S.C. § 552(b)(7)(E).

If you are dissatisfied with my action, an appeal may be made pursuant to 28 C.F.R. § 16.9 by writing to the Director, Office of Information and Policy, U.S. Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001, within 60 days from the date of this letter. Both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal." In the event you are dissatisfied with the results of any such appeal, judicial review will thereafter be available in the district where the requester resides or has a principal place of business, or in the United States District Court for the District of Columbia.

Sincerely,

[redacted]

Barbara Bush
Acting General Counsel

Enclosure

[redacted]

Security Awareness Tips

Your Golden Ticket... to Getting Scammed!

Beware of emails that promote investing in gold – scammers are exploiting the recent increase in gold's value (a prevalent media topic). Recent concerns about inflation and other economic issues have caused some investors to turn to gold as a safer investment. As a result, security organizations have noticed an influx of hoax emails that request users' personal information. In one such scam, the email's subject line reads, "Is Gold Your Ticket To A Golden Future?" and a "FREE investor kit" is offered to users who provide their contact information.

[redacted]

"Certain personalities are used in the image for this spam campaign including Glenn Beck. A Google search reveals an interesting article about Glenn Beck promoting gold investments. It seems that the spammer did some research in order to know about the association before propagating this spam campaign" (Hartnett, www.symantec.com).

Contributing sources: www.net-security.org; www.symantec.com; www.nytimes.com

User Awareness Tips

Thumb-thing's Fishy... Thumb Drive Safety 101

Removable devices such as thumb drives (also known as USB sticks) pose a unique challenge to Federal IT Security. While they are convenient, portable and great for storing files, they are also easy to lose, and are often used to spread malware.

The US-CERT (Computer Emergency Response Team) recommends the following measures to protect thumb drive data:

•Do not plug an unknown USB drive into your computer -- If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). *Do not plug it into your computer to view the contents or to try to identify the owner.*

•Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.

•Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

Contributing sources: www.us-cert.gov; news.cnet.com

About the JSOC Newsletter

The Justice Security Operations Center (JSOC) ***News You Can Use*** **Newsletter** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily - at work, at home, and virtually everywhere in between - and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email us at dojcert@usdoj.gov.

Cyber Awareness Tip

Cybersecurity Myth:

"Once software is installed on your home computer, you do not have to worry about it anymore."

- Vendors may release updated versions of software to address problems or fix vulnerabilities. You should install the updates (on your home computer) as soon as possible; some software even offers the option to obtain updates automatically.

Source: US-Cert

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Work from Home

Working from home when possible, as well as utilizing an Alternative Work Schedule (AWS) significantly reduces the energy and time spent commuting. Video and phone conferencing, and other workflow tools, make this an easy, effective alternative to traditional commuting.

Source: www.green-unlimited.com

News You Can Use

March 2011

Visit Our Website

Security Awareness Tips

Warning: Attackers May Attempt to Compromise Remote Access Tokens

A security breach at a vendor recently caused weaknesses in RSA SecurID tokens commonly used in remote access to Department systems. As a result, attackers may attempt to obtain users' PIN codes to access Department systems using RSA SecurID tokens.

By remaining alert for attempts to reset or obtain RSA SecurID token PIN codes, users can assist in keeping Department information secure.

All Department personnel are asked to:

- **Be cautious of messages, phone calls, or web pages requesting that you reset the PIN code used with your token.** Contact your component IT helpdesk if you receive an unexpected request to PIN code
- **Check the URL (address)** of web pages asking for to ensure they are legitimate government web pa imitations that look official.
- **Exercise caution** when OJJ1er1irlg contains links or att contains a sense of U.S. government e-mail

Please report suspicious messages to the Justice Security Operations Center (JSOC) by e-mail (DOJCERT@usdoj.gov) or phone (866-US4-CERT). Users may continue normal use of systems, keeping in mind the above requests to remain vigilant for attempts to obtain PIN codes. JSOC will distribute further information as it becomes available.

User Awareness Tip

Information Security 101: Avoid Password Reuse

In a recent study by the Security Group at the University of Cambridge Computer Laboratory, a comparison was conducted on two websites whose password information had been stolen. The websites had overlapping customers (based on email addresses), and of the customers who were registered at both sites, **76 percent used the same password on both accounts**.

Utilizing the same--or even very *similar*--passwords on multiple sites means that, if one account is compromised, they all are. Unfortunately, due to this common, insecure practice, "If a malicious hacker is able to get his or her hands on a user's password credentials for one domain, said hacker has a good starting point for figuring out the user's password for other sites" (Samson, *Infoworld.com*).

This issue is particularly relevant to Department of Justice users because, if an individual uses the same password at DOJ and non-work-related sites, they are not only jeopardizing their personal accounts, but also putting the Department's network at risk. At the very least, users should commit to never reuse their work-related passwords for any of their personal accounts.

Contributing Sources: Infoworld.com

The Justice Security Operations Center (JSOC) ***News You Can Use*** **Newsletter** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between-and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Reasons to be particularly careful when opening email attachments:

- Email is easily circulated - Forwarding email is so simple that viruses can quickly infect many machines.
- Email programs try to address all users' needs - Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.
- Email programs offer many "user-friendly" features - Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

Source: US-Cert

News Highlights

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Waste Less Paper

Whenever appropriate, re-use one-sided documents from a scrap paper bin in the same area as your printer or copier.

Source: Newdream.org

News You Can Use

February 2011

Visit Our Website

2011 DOJ Cybersecurity Conference

"Leveraging a Collaborative Defense"

The third annual DOJ Cybersecurity Conference was held February 8-9, with the theme "Leveraging a Collaborative Defense." This year's conference examined the changing threat picture and the new dynamics and challenges in defending DOJ networks. It also emphasized the need to work together to strengthen the Department's networks and applications security posture, while empowering its mission.

Thank you to all attendees -- particularly volunteers -- who helped to make this year's conference a success. Please remember to fill out your attendee survey so that your feedback can help shape next year's program. To request a specific topic be covered in a future conference, please email Jennifer Jones at jennifer.jones3@usdoj.gov.

Security Awareness Tip

What You Should Know About *Advanced Persistent Threat* (APT)

You may have heard the term "Advanced Persistent Threat" or "APT" in the news, usually referring to a determined group of hackers that continues to target computer users in an attempt to steal information over the long term.

Using methodical attack techniques employing targeted, malicious e-mail messages, the attackers trick users into opening a malicious attachment or clicking a link that leads to a compromise of sensitive information. ***Once inside an organization, the attackers quietly move laterally among network resources, elevating privileges and stealing information, persisting potentially for years without detection.***

The **Justice Security Operations Center** reminds users to remain vigilant for suspicious messages, keeping the following in mind:

- Attackers may send convincing messages appearing to come from a coworker, employer, or other reputable source to gain your trust.
- Be wary of any unsolicited message that requests you open an attachment or click a link, and attempt to confirm the authenticity of the message via phone.
- At home, employ updated antivirus software and educate others who share your computer that malicious e-mail messages can compromise your computer, and remind them to view unfamiliar e-mail messages with caution.
- Submit suspicious e-mail messages for analysis to JSOC via the e-mail address DOJMAIL-SPAM@usdoj.gov

Source: Infoworld.com

[redacted] treasure, they face. By contra[redacted] **there to stay as long as they can**. The attackers aren't trying to steal everything at once. Instead, they exploit dozens to hundreds of computers, logon accounts, and email users, searching for new data and ideas over an extended period of months and years."

Source: http://infoworld.com/d/security-central

About the JSOC Newsletter

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between - and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Good Security Habit: Lock Your Computer

Lock your computer when you are away from it by pressing the Windows Key and L. Even if you only step away from your computer for a few minutes, it's enough time for someone else to destroy or corrupt your information. Locking your computer prevents another person from being able to simply sit down at your computer and access all of your information.

Source: US_CERT.gov

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Green Lunch Ideas

Bringing lunch to work in reusable containers is likely the greenest way to eat at work, since ordering delivery and takeout usually leaves leftover packaging waste. If you do order delivery, join coworkers in placing a large order (more efficient than many separate ones). Also, bring in a reusable plate, utensils, and napkins.

Source: treehugger.com

[redacted]

You Can Use

January 2011

Visit Our Website

User Awareness Tip

Cyber Security Resolutions for 2011

Cyber security experts predict a rise in economic and job market-related scams in 2011; resolve to be extra vigilant in protecting yourself from cyber crime this year!!

Lottery and Sweepstakes Scams

According to the FBI's Internet Crime Complaint Center (IC3), consumers have reported a recent sweepstakes scam that sends emails and letters with fraudulent checks bearing the logos of financial services companies. Expect to see variations of these schemes in the coming year, using text messages and phone calls.

Employment Schemes

Both "get rich quick" and "work from home" schemes have become increasingly common, exploiting those facing difficult financial circumstances. "Common warning flags in postings for possible scams include: Inflated wages, vague wording or generic job openings, free training, guaranteed placement, no special skills or experience required, P.O. Box or out-of-state address, and job listings for government, civil service and overseas positions.".

[redacted]

Social Networking Dangers

Social networking sites are consistently risky, and threats are predicted to increase in 2011. They "provide an avenue of easy attack to users who are willing to click on every link they receive". Be sure to contact friends before clicking links, videos, etc., to ensure they are legitimate.

Sources: Dark Reading; Net Security; PC Tools

Security Awareness Tips

Information Security during International Travel

All federal employees embarking on international travel-whether work-related or not-should keep the following tips in mind:

Assume You're a Target, Because You Probably Are

"Travelers need to know that in light of current worldwide political and economic instability, the fact that they are American citizens and, in particular, U.S. government employees or contractors, makes them a target for exploitation".

Avoid Processing and Transmitting Sensitive Information

Travelers should assume that their transmissions are being intercepted and read anywhere networks are controlled by a foreign government. "Foreign network providers can disable mobile device encryption and then turn it back on after information is intercepted".

[redacted]

Power Down When Possible

Travelers should turn their mobile devices off when not in use in order to limit the potential for compromise. It is best to also remove the battery and SIM card, and store them separately from the device.

Steer Clear of Cafés

Internet cafés are NOT a safe alternative to utilizing your own electronic devices. The computers at many such establishments have malicious software that can capture passwords, bank account or credit card information, and the like. *Never* use cafés for official business.

Be Responsive

In the case of a security incident, know the proper method to report tampering, unauthorized use, loss or theft of IT media to your Component's IT Security Staff.

Contributing Sources: MacAfee; GCN

About the JSOC Newsletter

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between-and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Cyber Security Myth: *Attackers only target people with money.*

Truth: Anyone can become a victim of identity theft. Attackers look for the biggest reward for the least amount of effort, so they typically target databases that store information about many people. If your information happens to be in the database, it could be collected and used for malicious purposes. It is important to pay attention to your credit information in order to minimize any potential damage.

Source: www.us-cert.gov

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Environmentally Conscious Travel

When feasible, make it a habit to take the train, bus, or subway during business travel, instead of a rental car. If you must rent a car, opt for hybrids and other high-mileage vehicles, which some rental agencies now offer.

Better yet, utilize videoconferencing and other technological solutions that can reduce the amount of employee travel when possible.

Source: Sierra Club

[redacted]

Security Awareness Tips

'Tis the Season... to Get Scammed!

The hustle and bustle of the holidays-- with shoppers looking for great deals in a hurry-- provides an excellent opportunity for cyber criminals to strike. Don't be fooled by the common scams below:

[redacted]

Free iPad Offers

With Apple products being in high demand this season, lots of phony offers for free iPads and other merchandise are circulating online. Some users receive spam email messages that offer a free iPad with an online purchase. Those who attempt to make a credit card purchase receive neither the product they supposedly paid for, nor the free iPad they were promised, and their account information is in the hands of cyber criminals. Others have encountered quizzes on Facebook and Twitter that promise a free iPad in exchange for answering a few questions. To receive their final results, individuals must enter their cell phone number, which automatically subscribes them to a cell phone scam that charges their account $10 a week. Malicious links and other counterfeit offers for iPads are also common on social networking sites.

"Help! I've Been Robbed" Scam

This scam appears in the form of phony distress messages from someone you know, claiming they are out of town and in need of money immediately. Do not fall prey to the messages's sense of urgency-- first, call or email the supposedly stranded friend in order to verify their claims. Chances are, they're fine and you've encountered a scam.

Fake Gift Cards

Cyber criminals use phishing scams with offers of free gift cards to steal users' personal information and money. The offers can appear as pop-ups, emails, banners on web pages, and more. "The ruse may say something like 'The first 200 people to 'Like' [insert well-known retailer] on Facebook will receive a $500 gift card.' Then, to claim the prize, you have to enter personal information or take a bunch of online quizzes. The personal information is used for identity theft purposes, and the quiz results are sold to marketers, netting the crooks even more money".

[redacted]

Charity Scams

With increased giving, comes increased swindling. When considering donating to a charity online, remember to:

- Carefully check the name of any charity: Charity scams use names similar to the original charity in order to cause confusion and obtain your donations, i.e., National Cancer Society (scam) instead of American Cancer Society (legitimate).
- Check the email address of any message from a charity. Charities sending out emails should have top level domains like .org, .com, or .net and the email should come from this domain, not a free provider like hotmail or gmail. However, as a general rule *reputable charities don't spam and you won't receive an email from them directly without your prior inquiry.*

[redacted]

Contributing Sources: ftc.gov; newsroom.mcafee.com; eldergadget.com

About the JSOC Newsletter

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily-- at work, at home, and virtually everywhere in between--and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Power Surge Protection

Inclement winter weather is headed our way— keep your home PC safe from power surges and outages by:

- Investing in a power strip that protects against power surges; many strips advertise compensation if they do not effectively protect your computer.
- During a lightning storm or construction work that increases the odds of power surges, consider shutting your computer down and unplugging it from all power sources.

Source: US_CERT.gov

[redacted]

VPR Alerts
Security Advisories
Monthly Wrap-Up

Green Tip of the Month

Green Holiday Decorating

When decking your halls this season, keep these green tips in mind:

- Reuse decorations from year to year to save money and prevent unnecessary waste.
- Buy energy-efficient lights, such as LEDs, and put them on a timer so they aren't glowing hours longer than necessary.

Source: earth911.com

-News You Can Use

November 2010

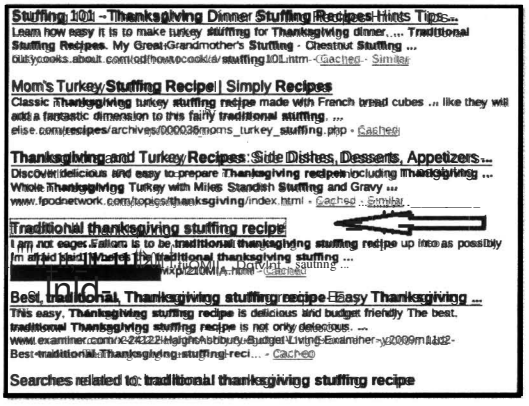
Visit Our Website

Security Awareness Tips

Thanksgiving Threats

While planning parties, printing out invitations and finding new recipes, many people forget to be particularly careful browsing the Internet around the holidays. Be aware that cybercriminals are utilizing search results for common holiday terms to attack unsuspecting users. Internet searches for "Turkey," "Thanksgiving," "Invitations" and "Printable (cards)" often yield malicious search results that redirect users to fake antivirus sites. Once downloaded, the software will do "a number of annoying things, such as hijacking web browsing sessions, repeatedly playing messages over the speakers (E.g. 'Your computer is infected'), and generating popups".

What is Fake Antivirus?
A fake antivirus is a warning message that pops up from a Web site and claims the user's computer is currently contaminated or not running properly. Also called "rogue antivirus" and "scareware," fake antivirus is a dishonest attempt to cause a user to purchase antivirus, registry cleaner or some other software that repairs problems or enhances performance.
Source: pcmag.com



It is important to examine any link before clicking it to make sure the URL is related to the search you conducted. While this does not guarantee the site is safe, it is a good preventative measure that can help you steer clear of malicious links. The best solution, however, is to type the specific URL of your intended destination in the address bar rather than conducting broad searches. "By manually typing the URL in the address bar, you can verify the information that [your web browser] uses to access the destination Web site. To do so, type the URL in the Address bar, and then press ENTER".

If you encounter an anti virus pop-up, immediately close your browser to avoid unintentionally downloading the malware, and contact your Component's IT security staff immediately.

Contributing Source: pandasecurity.com; microsoft.com

Fake USAA Phishing E-mails

A recent phishing scam has used the name of the United States Automobile Association (USAA) to lure victims into handing over their credit card information. Recipients of the email are asked to click a link to fill out a "new version of USAA Confirmation Form." Once they click the link, they are redirected to a phishing page with a fake form (see image at right) requesting their online ID, password, name, e-mail, USAA card number, expiration date, security code and PIN.

There are several warning signs indicating this is a scam, however: a small mistake in the wording of the message, the use of shortened links (to hide the actual destination URL), as well as a browser warning that there might be a problem with the destination URL.

Contributing Source: net-security.org

This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-357-0266

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between—and we provide the information you need to know, in terms you can understand. If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Safe Online Shopping

- **Use anti-virus software, a firewall, and anti-spyware software.** These are your first defense against viruses, etc.
- **Do business with reputable vendors.** Verify that the vendor is reputable and established before providing any personal or financial information.
- **Be wary of emails requesting information.** Legitimate businesses will not solicit account or personal information through email.

Source: US CERT

VPR Alerts
Security Advisories
Monthly Wrap-Up

Green Tip of the Month

Smarter Recycling Dos and Don'ts

- **Don't crush cans.** This is no longer necessary for processing.
- **Don't thoroughly clean every empty jar.** Machinery at the recycling center will clean jars.
- **Do sort recyclables.** Some recycling centers throw out recyclables that are not sorted.
- **Do recycle glossy paper.** Most centers now accept magazines.

Source: bestgreenhometips.com

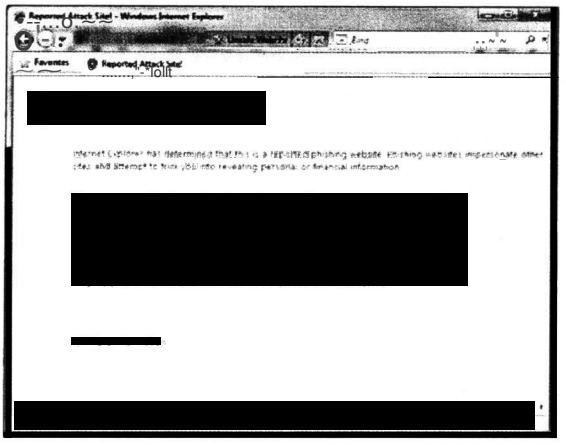
[redacted]

Visit Our Website

Security Awareness Tip

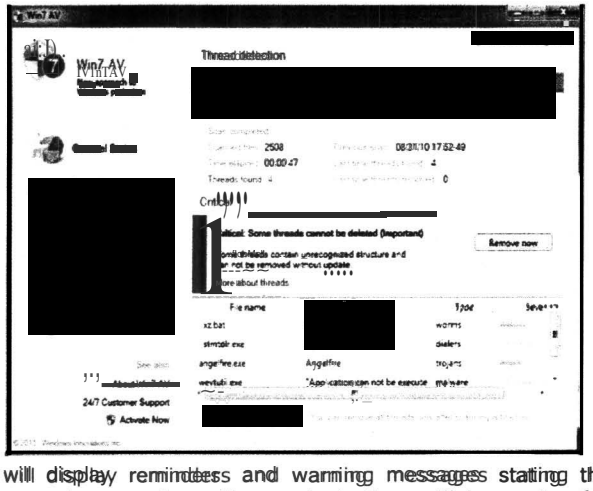
"MSIL/Zeven" Affects Internet Explorer, Chrome, and Firefox

A new fake anti-virus scam in the form of a browser warning page has been spotted by the Microsoft Malware Protection Center. The rogue, dubbed "MSIL/Zeven," has been spotted on various compromised websites, and is able to detect whether Internet Explorer, Chrome, or Firefox is being used, then generate a malware warning page very similar to those displayed by the respective browsers (See phony Internet Explorer page below).



It is important to note that all "the 'updates' point to a copy of MSIL/Zeven that promises to provide 'a new approach to windows detection,' but **Internet Explorer, Firefox, and Chrome do not offer such a solution when a website is blocked**" (Microsoft Malware Protection Center). Additionally, many of the pages have obvious grammar and spelling mistakes, such as "Get me our of here" (instead of "out") in the Firefox warning page, and "Proven antivirus protection fim one click" (rather than "im"). If you encounter such a warning page, hit Alt-F4 on your keyboard, which will immediately kill the browser (Select "Cancel" if a dialog box appears), to avoid unintentionally downloading the malware, and contact your Component's IT security staff right away.

If a user clicks the "Update Now" or "Upgrade" box on the page, their computer will be infected and the phony "Win7 AV" product will be installed. It starts by conducting a fake scan, indicating that it has found malicious files, infections, and the like. While the scan appears legitimate (see image at left), it does not actually inspect the user's computer, and the report it generates is completely false; "the features don't work; everything is there just to look nice, not to offer any kind of protection (just like in all other rogue antivirus programs)" (Microsoft Malware Protection Center). After the initial scan, the user is informed that the program has detected various problems, but cannot eradicate them unless they upgrade to the full version of the program (i.e. pay money). Even if the user chooses *not* to purchase the product, the MSIL/Zeven malware is already on their PC and will display reminders and warning messages stating that the computer is infected. If the user does purchase the product, they will be paying for an ineffective scammer, and their credit card information will be in the hands of cyber criminals.



Contributing Source: www.blogs.technet.com/b/mmpc/

*****This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.*****

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between -- and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.j.jones3@usdoj.gov

Cyber Awareness Tip

"Free iPhone" Facebook Scam

Beware of iPhone-related status updates from friends on Facebook, with claims like: "Just testing Facebook for iPhone out :P Received my free iPhone today, so happy lol... If anyone else wants one go here: (link))". Users who click on the link are asked if they want to "Allow" the application to access their basic information. Clicking "Allow" enables the application to access users' personal information, as well as to post on their wall. Each click earns commission for the scammers. Impacted users should immediately delete references to the free iPhone from their wall, and remove the offending application from Account/ Application Settings.

Source: www.net-security.org/secworld

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Switch out your disposable plastic hand soap containers for refillable hand soap pumps. Most brands offer bulk soap refills, and you will be saving both money and landfill space!!

Source: www.bestgreenhometips.com

[redacted]

News You Can Use

September 2010 *Visit Our Website*

JSOC Issues Two Alerts to DOJ Computer Users

Computer "Worm" Attacks Federal Agencies

A new computer "worm" attacked several federal agencies and Fortune 500 companies yesterday. The malicious email messages contain the subject line "Here You Have" or "Just For You" and contain a link to a seemingly legitimate PDF file. If a user clicks on the link, they will be redirected to a malicious website that will prompt them to download and install a screensaver (.scr) file. If they agree to install this file, they will become infected with an email worm that will continue to propagate through their email contacts (see Computer Worm definition above).

Computer Worm:
A software program that is designed to copy itself from one computer to another, without human interaction. Unlike a computer virus, a worm can copy itself automatically. Worms can replicate in great volume. For example, a worm can send out copies of itself to every contact in your e-mail address book, and then it can send itself to all of the contacts in your contact's e-mail address books (Microsoft.com).

The Department of Justice received over 200 of these emails but the Justice Security Operations Center (JSOC) activated the OCIO Incident Response Action Team and blocks were instituted at the TIC Internet gateways. Additionally, Components were required to update all antivirus products in use, which minimized our exposure to only six infected machines. Even though [redacted] the Department is now protected, sometimes the adversaries change the email to look slightly different so they can get past defenses.

The Department asks that all users carefully watch their emails, both at work and on their home machines.

Attackers Attempt to Access Department Systems Through Malicious E-mail Messages

The Justice Security Operations Center (JSOC) [redacted] designed to give attackers remote access to Department systems. Due to the recent increase and nature of these targeted intrusion attempts, we urge users to be extra cautious when opening e-mail messages at work and at home.

Typically, users will receive a malicious message disguised as a legitimate e-mail containing links or attachments, often referring to U.S. government information, reports, conferences, or meeting agendas. If a user clicks the link or opens the attachment, the attacker can gain full control of their workstation and information.

To reduce the risk of compromising your DOJ workstation, be alert for unsolicited e-mail messages and keep in mind the following traits common to malicious e-mail messages:

- Subject matter related to recipient's work, possibly containing actual U.S. Government information
- A sense of urgency to convince the recipient to open an attachment or click a link within the message
- Convincing content such as upcoming meeting agendas, reports, information on current events or policy issues
- Seemingly legitimate sender (government and commercial addresses, including @usdoj.gov) using legitimate signature and contact information
- An attachment (typically a .pdf or .zip file) or link

The Justice Security Operations Center would like to examine suspected malicious e-mail messages. To preserve the hidden message information typically invisible to average users, suspicious e-mail messages must be sent to JSOC in a certain way. To forward a message for analysis, please follow the instructions available on JSOC website: http://dojnet.doj.gov/jmd/irm/itsecurity/documents/malicious_email_submittal.pdf.

This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between -- and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Safe Online Gaming at Home

- Be careful when downloading free to play (F2P) clients on your home computer. If the client software is malicious, you could be putting your PC at risk.
- Don't give out your login information to strangers. In fact, don't give out ANY kind of information, personal or not, to people you meet gaming.
- Avoid falling for the old "FarmVille Secrets" scam. You will either download a Trojan or expose your Facebook login info to criminals.

Source: www.gizmodo.com

[redacted]

Green Tip of the Month

Think Before You Print

- Ask yourself: could this be read or stored online instead? Make it a policy to post employee manuals and similar materials online, rather than distribute print copies. They're easier to update that way too.
- Request to be removed from mailing lists before you recycle unwanted mail.

Source: www. sierraclub.typepad.com

[redacted]

News You Can Use

Visit Our Website

Security Awareness Tip

Increase in Social Networking Scams

In its presentation to the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security last month, the FBI reported a significant increase in the use of social networking accounts in Internet scams. Gordon Snow, Assistant Director of the FBI's Cyber Division, stated, "The surge in the use of social networking sites over the past two years has given cyber thieves and child predators new, highly effective avenues to take advantage of unsuspecting users" (www.networkworld.com).

A couple common tactics used on social networking sites include:

- **Data Mining**, in which cyber criminals extract bits of information about victims and then use it to scam them. A common example is a "getting to know you quiz" on a social networking site; "While the answers to these questions do not appear to be malicious on the surface, they often mimic the same questions that are asked by financial institutions or e-mail account providers when an individual has forgotten their password" (www.networkworld.com). Scammers can thus gain information that will allow them to access the victim's email, bank accounts, etc. Additionally, collecting personal information is made even easier because many users "often accept into their private sites people that they do not actually know, or sometimes fail altogether to properly set privacy settings on their profile" (www.networkworld.com). Friends of friends should not be able to view your birthday, cell phone number, or any other information that could be used to impersonate you to credit card companies, credit unions, etc.

- Data mining can be applied in **Phishing**, in which cyber criminals attempt to acquire passwords, account numbers and other sensitive information by pretending to be someone else, often through personalized, legitimate-looking messages. One example is a warning message that appears to be from your bank, requesting you submit your account information for verification purposes (note that most banks will not contact you via email to gather information). A recent phishing scam that has plagued Facebook and other social networking sites is the "Help, I am stranded!" scam, in which victims receive a message appearing to be from a friend, claiming they have been robbed of their credit cards, passport, money, and cell phone, and are in immediate need of money. While the simple solution to this scam is to call the supposedly stranded friend in order to verify their claims, many users fall prey to the message's sense of urgency and send money. Phishing scams can be found in messages, links, or videos (appearing to be from friends) within the site, or emails sent to users claiming to be from the social networking site itself.

[redacted]

With the growing number of social networking scams– annual crime complaints have increased 667.8% between 2001 and 2009– it is important to utilize social networking sites' privacy settings, browse cautiously and contact the message sender before clicking anything.

Contributing Sources: www.networkworld.com Image: www.gizmodo.com

[redacted]

User Awareness Tip

Warning: DOJ Users Targeted in Parking Permit Phishing Scam

A number of Department of Justice users received an e-mail message disguised as a [redacted] with an attachment [redacted]. The attachment is not a [redacted], but instead redirects users to a site containing malicious software. If you encounter a message of this nature, DO NOT open the attachment, and contact your Component's IT security staff immediately.

This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily– at work, at home, and virtually everywhere in between– and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

"Keep Me Signed In" Box

- If you are not on your personal laptop or home computer, DO NOT select the "Keep me signed in" box on websites.
- Although your work computer may feel like it belongs to you, a snooping co-worker could easily open your browser and access your accounts if you stay signed in.
- If you sign in to a particular site, do not just navigate to another page or close the browser-be sure to sign out as well.

Source: www.gizmodo.com

[redacted]

Security Advisories
Monthly Wrap-Up

Green Tip of the Month

Water Conservation

Be sure to turn off faucets completely, ensuring that they don't drip. A faucet, leaking at a rate of only one drop per second, can waste more than 25 liters of water a day – that's about 10 000 liters a year.

Source: www.about.com

[redacted]

Visit Our Website

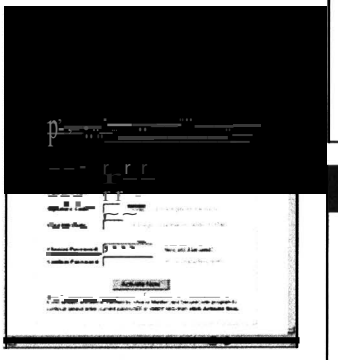
Security Awareness Tip

Zeus Botnet Incarnated to Exploit Credit Card Verification Services

The Zeus botnet, a Trojan horse that steals banking information, social networking logins, and email accounts, was first seen in July 2007, and has been widespread since June 2009. Zeus is particularly difficult to identify, because it is reconfigured more often than most malware, due to its creators "...allowing other cybercriminals to license the rights to use the malware. As a result, there are many different gangs running their own licensed versions of Zeus and distributing them independently" (SC Magazine).

[redacted]

As you may recall, Zeus resurfaced early this year as a series of emails targeting Federal employees. The messages appeared to be from a reputable CIA figure and warned against a Russian phishing attack, then encouraged recipients to install a "Windows update" to protect their computers.



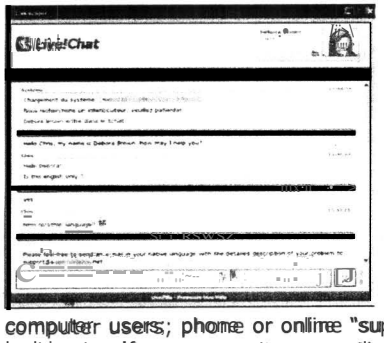
The most recent incarnation of Zeus, however, poses as a credit card verification page. Once downloaded, the malware waits for the user to visit a bank website, then emerges (appearing to be associated with the bank) and asks the victim to fill out an enrollment form for the Verified by Visa or Mastercard SecureCode programs. The phishing page states that "Due to recent changes in FDIC Deposit Insurance Rules, all our customers must be enrolled in the Verified by Visa or MasterCard SecureCode program depending on type of your check card." Once the customer submits their information, the data is used to register accounts with the verification services and perform fraudulent transactions.

With 15 US financial institutions affected and an estimated 1 in every 100 computers infected, this has become a widespread problem. If you encounter an unexpected Visa or Mastercard verification page, it is recommended you close your browser and contact your bank regarding the issue.
Contributing Sources: www.v3.co.u; www.scmagazineus.com

User Awareness Tip

Fake AV Vendors Offering "Live Support"

Fake Anti Virus software or "Fake AV" consists of phony alerts or warnings that typically pretend to scan a victim's computer, then claim to find some form of malware and seek payment from the victim to remove the (non-existent) problem.



As if this scam wasn't deceptive enough, some fake AV developers are now offering "live support" to users, in order to convince potential victims of the legitimacy of their products. Research found that there was in fact a person – not a bot– responding to questions about the product, and "They are offering support by email, chat, and phone and are very well organized. You can get uninstallers for older variants of their product, and also trial versions for their newer products" (www.securelist.com)

Remember that scammers are constantly honing their attacks to ensure they victimize increasing numbers of computer users; phone or online "support" does not prove a particular antivirus software is legitimate. If you encounter an anti virus pop-up, immediately close your browser to avoid unintentionally downloading the malware, and contact your Component's IT security staff immediately. *Contributing Source: www.securelist.com*

*****This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.*****

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between– and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Safe Internet Publishing

Although people are typically wary of sharing personal information with strangers they meet on the street, they may not hesitate to post that same information online. Before posting information online, remember to:

- View the internet as a novel, not a diary: assume that people you have never met will view the information you are publishing.
- Think ahead: once you publish something online, it cannot be taken back. It is available to other people and to search engines, and may never be completely removed.

Source: US_CERT.gov

[redacted]

VPR Alerts
Security Advisories
Monthly Wrap-Up

Green Tip of the Month

Reduce E-Waste

The world generates 20 to 50 million metric tons of e-waste, which makes up 2 percent of solid waste in the U.S. and is the fastest-growing segment of U.S. garbage. Be sure to take old electronics and computers to your local facility along with your usual recycling.

Source: www.pcmag.com

News You Can Use

June 2010

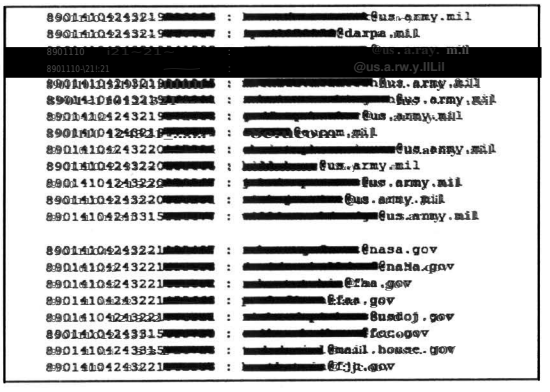
Visit Our Website

Security Awareness Tip

AT&T Security Breach Impacts iPad Users

Early in June, just two months since the release of the Apple 3G iPad, AT&T was made aware of a breach that exposed the email addresses and associated AT&T network authentication IDs (known as ICC-IDs) of thousands of iPad owners --many of whom are Federal employees. A group of security researchers called "Goatse Security" (whose motives are currently in question) discovered the flaw and extracted 114,000 email addresses before spreading word of the problem. Goatse Security has been accused of informing outside parties of the hole before AT&T had patched it, potentially allowing hackers to access more iPad users' email addresses. In its defense, a Goatse Security representative stated that "We did not contact AT&T directly, but we made sure that someone else tipped them off" before spreading word of the hole. They also stated that they were not paid for disclosing information to third parties. AT&T closed the hole shortly after being notified, but an FBI investigation is currently underway to determine whether illegal activity was involved in the attainment of the email addresses.

According to an article from arstechnica.com, "...the worst consequences of this particular leak are most likely increased spam sent to or spoofed as coming from a particular e-mail address. However, it's not entirely unreasonable to suspect that hackers might attempt to crack into some of the e-mail accounts revealed, which include officials from the FCC, FAA, NASA, and the Army." If you own an iPad, there is a possibility that your email address has been made public through this breach, and it is recommended that you remain particularly vigilant when checking email. If you encounter a message that may be an intrusion attempt or pose a threat to DOJ computer security, please follow the instructions for reporting malicious email at JSOC's DOJNet website: http://dojnet.doj.gov/jmd/irm/itsecurity/documents/malicious-email-submittal.pdf



Contributing Sources: www.arstechnica.com;; www.gawker.com; http://security.goatse.fr/

User Awareness Tip

Protecting Your PC from Spyware and Adware

Spyware and Adware are types of software that, when installed on your computer, may send you pop-up ads, redirect your browser to certain web sites, or monitor the web sites that you visit. The presence of spyware is typically hidden from the user, but some indications that it is installed on your computer are:

- Endless pop-up windows or Windows error messages
- New, unexpected toolbars in your web browser
- Your browser's home page changed
- Your computer suddenly seems very slow when opening programs or processing tasks

Whether or not you suspect Spyware is installed on your computer, it is wise to run anti-virus software and to adjust the settings so that you are periodically reminded to run a full scan.

Contributing Sources: www.US-CERT.gov

This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.

**Questions regarding this newsletter or requests for permission to redistribute should be directed to: JSOC 202-307-5332*

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily-- at work, at home, and virtually everywhere in between—and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Removing Personal Information from Old Cell Phones

Before disposing of an old cell phone, it is important to ensure your personal information has been removed. A recent study of 2,000 recycled cell phones found that 99% of them had personal data still stored in them, including sensitive material like bank account information. Before getting rid of your phone, be sure to:

- Notify your cellular provider and terminate service on your phone.
- Remove your SIM card-- the tiny card inside your phone, which contains data stored in your phone.
- Erase all the history from your phone through a hard reset.

More information on performing each of these steps can be found in your phone's user manual.

Source: www.planetgreen.discovery.com

VPR Alerts
Security Advisories
Monthly Wrap-Up

Green Tip of the Month

Green Packaging

When shopping, choose products with smarter packaging-i.e., less packaging and use of eco-friendly materials-- and write to let manufacturers know when you don't like their packaging.

Source: the Daily Green

[redacted]

News You Can Use

May 2010

Visit Our Website

Security Awareness Tip

DOJ SPAM Mailbox

The Justice Security Operations Center (JSOC) provides the DOJMAIL-SPAM mailbox to allow reporting of e-mail messages that users suspect may be an intrusion attempt or a threat to computer security. JSOC analyzes messages sent to this mailbox and develops mitigation and detection methods to help protect Department systems from intrusions.

There are specific instructions that need to be followed when forwarding suspected malicious e-mail messages to JSOC for further analysis, which are online at JSOC's DOJNet website: http://dojnet.doj.gov/jmd/irm/itsecurity/docs/emailsmalicious-email-submittal.pdf.

Please note that JSOC does not analyze or block spam or other nuisance messages, unless they pose a threat to computer security.
If you would like to block spam, nuisance, or other non-malicious e-mail messages, several options exist:

1) Contact your component IT Helpdesk for information on the Proofpoint Mail Digest and end-user mail filter settings. When enabled by your Helpdesk, this service provides end-users with the ability to manage spam settings, including blocking specific e-mail addresses, **OR**

2) Contact your component IT helpdesk for information on how to block specific senders within your e-mail application using built-in tools (e.g., "Junk E-mail" filtering in Microsoft Outlook)

User Awareness Tip

Cyber Attacks Center Around 2010 World Cup

The FIFA World Cup 2010, like most events that receive heavy media coverage, has provided cyber criminals the opportunity to attack unsuspecting computer users in various ways. Using hacking techniques, attackers have managed to have their malicious sites listed in the top Google search results. As seen in the image below, the ***top four results*** --out of over 17,000-- for a World Cup-related query led to malicious websites. Clicking on any of the top results causes a phony "Windows Security Center" notification to pop-up, a common Fake AntiVirus technique. Users need to be cautious when conducting popular searches, and immediately close their browsers if they receive a supposed "antivirus alert." (For more information on Fake AV attacks, see the February 2010 issue of *News You Can Use*.)

Cyber criminals are also sending out emails with malicious PDFs, claiming the attachments contain free World Cup tickets or a World Cup Travel Guide. Users should use their better judgment when faced with offers that are unsolicited and/or sound too good to be true, and refrain from opening such attachments.

Contributing Sources: ESET Threat Blog; NetworkWorld.net

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between -- and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Protecting Personal Information

As long as you have a computer and connect it to a network, you are vulnerable to someone or something else accessing or corrupting your information. To minimize your risk, adhere to the following rules:

- Lock your computer when you are away from it.
- Disconnect from the Internet when you are not using your computer.
- Check your computer's security settings to make sure they meet your needs.
- Back up all of your data.

Source: www.US-CERT.gov

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Top Three Office Pet Peeves Resulting in Increased Waste:

- Mindless, unnecessary printing
- Leaving lights on
- Lack of recycling bins

Source: the Daily Green

[redacted]

News You Can Use

April/2010

Visit Our Website

Security Awareness Tip

DOJ Continuous Monitoring Initiative

DOJ is in the process of moving to a model of continuous monitoring of assets, vulnerabilities, configuration changes, and threats in order to fulfill operating requirements, minimize risk exposure, and improve computer incident response. The Department's current risk management model focuses largely on "snapshots" provided by periodic assessments and audits. This model is not only reactive, but the operating environment is also ever-changing, resulting in security assessments that are quickly outdated and lack a real-time evaluation of risk.

[redacted]

Due to this deficiency, DOJ made the decision to implement Enterprise Lifecycle Management System (ELMS) BigFix. This technology will provide situational awareness and greatly improve our current risk management methods. Continuous monitoring will provide real-time asset inventories and endpoint visibility to the Department through a centralized management console. DOJ Components, OBDs, and system owners will also have their own console to monitor and evaluate system vulnerabilities to determine applicability within their environment. Having an accurate understanding of DOJ's security posture will enable us to assume greater risk levels when appropriate. Additionally, new FISMA reporting guidelines were released last week, which require changing to automated data feeds, and ELMS supports these new requirements.

Continuous monitoring technology will allow decision makers access to key information quickly and efficiently, and streamline Department compliance reporting. DOJ will now be able to fulfill data calls within hours --rather than weeks or months-- while eliminating the uncertainties of self-reporting.

User Awareness Tip

Post-Tax Day Email Scams

April 15th has passed, and many taxpayers are anxiously awaiting their returns. Not surprisingly, hackers are seizing the opportunity to scam as many users as possible by sending out fraudulent emails marked as notifications from the Internal Revenue Service (IRS). Many of these emails claim that taxpayers must submit financial information such as bank account and credit card numbers, passwords and ATM PINs in order to receive their returns. Some are intended to frighten taxpayers by claiming to come from the IRS' "Fraud Department." Others state that taxpayers will receive money for filling out a customer satisfaction survey. It is important to note that *the IRS does not initiate taxpayer communications through e-mail.*

Department of the Treasury
Internal Revenue Service

If you encounter an unsolicited tax-related email from the IRS:

- Do not reply.
- Do not open any attachments.
- Do not click on any links.

Click here for a list of the top-12 IRS scams of 2010.

Contributing Source: www.IRS.gov

This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.

Questions regarding this newsletter or requests for permission to redistribute should be directed to:
JSOC 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between -- and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Email Attachment Safety

An email attachment is a computer file that is sent along with an email. Attachments are convenient, but they can also carry viruses. Follow the tips below to protect yourself:

- Be wary of unsolicited attachments, even from people you know.
- Keep software up-to-date in order to minimize your vulnerability.
- Turn off the option to automatically download attachments.

Source: www.US-CERT.gov

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Go as Paperless as Possible!

- Keep copies of important emails; files, manuals and more on your computer
- Review any documents online instead of printing them out.
- Send company updates through email instead of on paper.

The Daily Green

[redacted]

March 2010 *Visit Our Website*

Security Awareness Tip

Operation Aurora

Mid-December 2009, hackers initiated a highly sophisticated attack on Google and more than twenty other companies, with the goal of accessing source code and gathering information about dozens of U.S., Chinese and European users who were advocates of human rights in China. A combination of encryption, stealth programming, and exploitation of a previously unknown ("zero-day") vulnerability in Microsoft Internet Explorer allowed hackers entry into two Gmail accounts, but Google claims the access was limited to account information rather than actual email content. Upon investigating further, however, Google discovered that hackers had successfully gained entry into targeted Gmail accounts via phishing scams and malware on the users' computers. The attack was tentatively linked to China due to the presence of an obscure algorithm in the malware, which had only been published in Chinese and was virtually unknown outside of China.

References in the malware to a file folder named "Aurora," earned the attack the name "Operation Aurora." The incident has resulted in considerable contention between Google and China, with Google refusing to continue censoring certain search results on its Chinese search engine, stating "...these attacks and the surveillance they uncovered—combined with attempts over the last year to further limit free speech on the web in China including the persistent blocking of websites such as Facebook, Twitter, YouTube, Google Docs and Blogger—had led us to conclude that we could no longer continue censoring our results on Google.cn" (*The Official Google Blog*). On March 22nd, Google announced on its blog that users visiting Google.cn are now being redirected to Google.com.hk, where they will receive uncensored search results, and which will "meaningfully increase access to information for people in China." China maintains that its Internet safety policy is transparent and consistent, and resents the U.S.'s accusation that it had any participation in the attack.

Operation Aurora serves as a cogent reminder to the general public to remain diligent on patching. Microsoft issued an out-of-band (outside the normal schedule) patch for Aurora on January 21, 2010, but as word of the Internet Explorer vulnerability spread, hackers scrambled to exploit it before users were protected. It is therefore crucial to apply patches as soon as possible; JSOC releases VPRs for software patches resolving vulnerabilities with a CVSS base score of 7.0 or above (as determined by the National Institute of Standards and Technology), and sets patch implementation precedence based on public exploitation of vulnerabilities, if applicable.

Contributing Sources: The Official Google Blog; Wired.com

****This document is intended for Department of Justice internal use only and is not to be distributed outside the Department.****

Questions regarding this Bulletin or requests for permission to redistribute should be directed to:
JSOC/DOJCERT 202-307-5332

What is the JSOC Newsletter?

About the JSOC Newsletter:

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between-and we provide the information you need to know, in terms you understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

A password is often the only barrier between other computer users and your personal information, yet most people create passwords based on personal information that could be guessed or easily cracked by a hacker. Follow these tips to create the most effective password:

- Do not use a password based on personal or easily accessible information.
- Do not use words that can be found in a dictionary of any language.
- Use a combination of letters, numbers and special characters.

Source: www.US-CERT.gov

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Energy-Efficient Lighting

Replace incandescent light bulbs with compact fluorescent light (CFL) or light emitting diode (LED) bulbs, which give off less heat than incandescents and last longer.

The Daily Green

News You Can Use

February 2010

Visit Our Website

DOJ Cyber Security Conference Recap

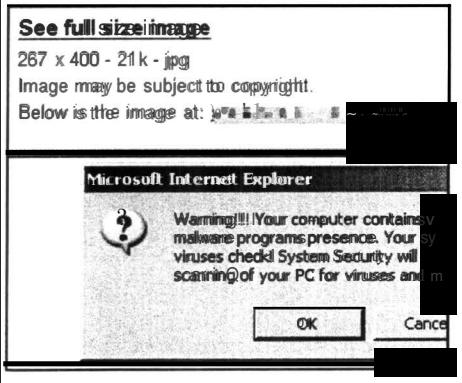
The 2010 Department of Justice Cyber Security Conference was held February 2-3, proving our largest turnout yet. This year's theme was "Keep Our Information Secure" and discussed new Department security initiatives, emerging technologies and security capabilities piloted by DOJ Components, as well as future direction of the Office of Management and Budget and the U.S. government. Thank you to all attendees -- particularly volunteers -- who helped to make this year's conference a success. Please remember to fill out your attendee survey so that your feedback can help shape next year's program. To request a specific topic be covered in a future conference, please email Jennifer Jones at jennifer.jones3@usdoj.gov.

Additionally, Components will have an opportunity to showcase their own security advances, measures and programs at next year's conference; Information Technology Security Staff (ITSS) will call for abstracts during the fourth quarter of the year and notify Components of their selection shortly thereafter.

Security Awareness Tip

Google Image Search Targeted by Fake AV Attacks

Anti-Virus fakealerts -- phony warnings that appear to indicate a virus scan is running on your computer and then insist you purchase a product to remove the supposed "infection" -- can now list Google image search as prey to their attacks. Until recently, Fake AVs were primarily located on Trojan Horse applications; however, due to the success of this particular attack, hackers have now migrated fakealerts to browsers.



As discussed in a *Webroot.com* blog, an image search for a television actress yielded phony image links leading to a supposed Microsoft Internet Explorer "warning" which stated that the user's system had been compromised (the typical Fake AV baiting tactic). Strangely, the Google search pane remains at the top of the page, while the fakealert runs in the lower section (see image at left).

Once the user clicks the fakealert, a rogue antivirus (with a name such as "Total Security" or "Security Tool") hides the desktop with its personalized wallpaper, interferes with the user's ability to right-click their mouse or use its scroll wheel, prohibits applications from running (including Internet Explorer), and blames all of the problems on an infection within the machine. The purpose of this elaborate Fake AV or "scareware attack" is to convince users to spend $50 to $90 on bogus antivirus software, contributing to the millions of dollars in profits generated by this scam to date.

If you encounter a fakealert, hit **Alt-F4**, which will immediately kill the browser (Select "Cancel" if a dialog box appears), to avoid unintentionally downloading the malware, and contact your Component's IT security staff right away.

Reference: Webroot Threat Blog

What is the JSOC Newsletter?

The Justice Security Operations Center (JSOC) ***News You Can Use Newsletter*** strives to protect readers against Internet cyber threats by keeping them up-to-date on the latest security issues, vulnerabilities, and computer user tips. The threats we address affect you daily -- at work, at home, and virtually everywhere in between—and we provide the information you need to know, in terms you can understand.

If there is a specific topic you would like to see discussed in a future newsletter, please email Jennifer Jones at jennifer.jones3@usdoj.gov

Cyber Awareness Tip

Losing a laptop or PDA means not only losing the machine itself, but sometimes the information on it. Follow the tips below to minimize damage:

- Password-protect your computer or PDA. Also, when entering your password, ensure that others are not able to view it by "shoulder surfing."
- Do not leave your device unattended.
- Downplay your laptop or PDA—avoid using it in public if possible.
- Back up your files.

Source: US_CERT.gov

[redacted]

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Ditch Dixie Cups

Rather than using a Dixie cup each time you make a trip to the office water cooler, bring your own cup and encourage colleagues to do the same—it saves loads of paper!

The Daily Green

News You Can Use

January 2010 *Visit Our Website*

Security Awareness Tip

JSRA

JSRA is a Virtual Private Network (VPN) which provides a secure and encrypted connection to Department of Justice information resources via the Internet and is part of the DOJ Disaster Contingency Plan.

- **When utilizing the JSRA network, users should follow best practices, DOJ Security Order 2640.2F, and DOJ General Rules of Behavior FY10.**
  - http://10.173.2.12/dojorders/doj2640.2f.pdf
  - http://10.173.2.12/dojorders/doj2740.1a.pdf
  - http://10.173.2.12/jmd/irm/itsecurity/documents/general_rob_fy10.pdf
- **DOJ guidelines for JSRA users:**
  - Do not connect personal computers to the JSRA Network.
  - Ensure the computer's software is fully patched and the virus protection definitions are up-to-date.
  - Do not use Peer-to-Peer (P2P) file sharing on the internet, such as instant messaging, Skype, BitTorrent, or eDonkey, etc. P2P is expressly forbidden throughout the Department unless a waiver is obtained from the Department's CIO or his designee in each Component.
  - Use only authorized thumb drives and diskettes, only download files from known and reliable sources, and employ virus-checking tools prior to use.
  - Do not allow family members access to your government laptop.
  - Government laptops are only permitted to connect to the internet through the JSRA network.

Exemption 7 (E)

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way - at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Malware Campaign Disguised as Swine Flu Messages

This campaign sends e-mail messages containing information regarding H1N1 vaccination programs, purporting to be from the Centers for Disease Control and Prevention (CDC). The fake messages attempt to entice recipients to click a link to a malicious file.

Users who click on this link may become infected with malware. Public reports indicate that the messages contain subjects including "Governmental registration program on the H1N1 vaccination" and "Your personal vaccination profile." Subject lines related to this malware campaign will likely change over time.

Click here for more information.

[redacted]

VPR Alerts

Security Advisories

Monthly Wrap-Up

Green Tip of the Month

Don't Dump, Donate

The next time you upgrade something, can no longer stand the sight of something hideous, or simply need to downsize, think "donate" instead of "dump."

The Daily Green

[redacted] News You Can Use

November 2009

Visit Our Website

Security Awareness Tips

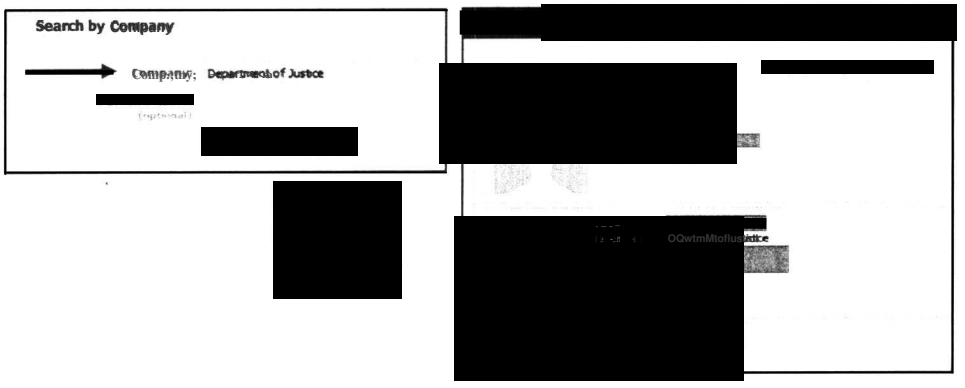
Hidden Dangers of the Web

Social Networking

Pro	Con
• Enables quick, efficient communication • Network with friends, coworkers, friends of friends, classmates, the world...	• Wide user base provides attractive target for attackers • Can unintentionally leak sensitive information

Facebook Targeting & Exploitation

- Facebook has a "search by company" feature to allow networking with coworkers. Over 500 profiles with DOJ listed as employer on Facebook.



- Allows adversaries access to your private life and information that can be used to target DOJ personnel.
- Your full name can be used to craft targeted e-mail messages or for other nefarious purposes.
- Facebook disabled numerous fake profiles that included a link to a purported video but which instead displayed a fake antivirus alert. Scam designed to get credit card information from victims for identity fraud purposes and install spyware.
- **Mitigation: Don't include place of employment on public profiles**

Drive-by Downloads

- Downloading malicious software without the user's knowledge by exploiting a web-based vulnerability
- Can occur while visiting legitimate websites (Facebook, personals, news, search engines)
- Poses security risk to Department by giving attackers remote access to systems
- **Mitigation: Limit personal use of the Internet while connected to a DOJ system to minimize exposure**

Contributing Source: JSOC CyberFest 2009: Emerging Threats Presentation

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

DOJ guidelines for JSRA users

- Do not connect personal computers to the JSRA Network.
- Ensure the computer's software is fully patched and the virus protection definitions are up-to-date.
- Do not use Peer-to-Peer (P2P) file sharing on the internet, such as instant messaging, Skype, BitTorrent, or eDonkey, etc. P2P is expressly forbidden throughout the Department unless a waiver is obtained from the Department's CIO or his designee in each Component.
- Use only authorized thumb drives and diskettes, only download files from known and reliable sources, and use virus checking procedures prior to use.

[redacted]

Security Advisory - DOS Attack (JSOC)
Security Advisory - RIM BlackBerry SW Update (JSOC)
October VPR Alerts (JSOC)

Green Tip of the Month

Turn your computer off at night

Shutting your computer off before going to bed each night will save an average of $90 worth of electricity per year.

The Daily Green

[redacted]

News You Can Use

September 2009

Visit Our Website

Security Awareness Tips

Five Ways to Meet Compliance in a Virtual Environment

Five steps for securing and locking down virtual environments and meeting compliance requirements:

1. **Platform Hardening** - Configure the virtualization platform, both the hypervisor and administrative layer, with secure settings, eliminate unused components, and keep up-to-date on patches
2. **Configuration and Change Management** - Extend your current change and configuration management processes and tools to the virtual environment
3. **Administrative Access Control** - Server administrators should have control over virtual servers and network administrators, over virtual networks, and these administrators need to be trained in virtualization software in order to avoid misconfiguration of systems
4. **Network Security and Segmentation** - Deploy virtual switches and virtual firewalls to segment virtual networks, and use your physical network controls in the virtual networks as well as change management systems. Be sure that machines handling protected data are isolated, and deploy virtual IDS/IPSes
5. **Audit Logging** - Monitor virtual infrastructure logs and correlate those logs across the physical infrastructure, as well, to get a full picture of vulnerabilities and risks. Adapt automated tools and SIEM systems to integrate logs from both environments

Contributing Source: Dark Reading

Computer User Tips

Parental tips to keep children safe online

- Keep your computer in an open area
- Set rules and warn about dangers
- Keep lines of communication open
- Consider implementing parental controls
- Consider partitioning your computer into separate accounts

Contributing Source: US-CERT Cyber Security Online

Keeping Laptops from Getting Lost or Stolen

Keep these tips in mind when you take your laptop out and about:

- Treat your laptop like cash
- Keep it locked
- Keep it off the floor
- Use a non-descript carrying case
- Keep your passwords elsewhere
- Password protect your system
- Backup important data before traveling

Contributing Source: StaySafeOnline.info

To view the latest JSOC Monthly Wrap-Up, visit our website at:
http://dojnet.doj.gov/jmd/irm/itsc/itsecurity/monthly_report.php

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way - at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Protecting Your Data

- Use and maintain antivirus software and a firewall
- Regularly scan for spyware
- Keep software up-to-date
- Evaluate your software settings
- Avoid unused software programs
- Create separate user accounts
- Establish computer use guidelines
- Use passwords and encrypt sensitive files
- Properly dispose of sensitive info

Contributing Source: US-CERT.gov

[redacted]

VPR Alert - Adobe Acrobat (JSOC)

VPR Alert – MS Critical Patches August 2009 (JSOC)

VPR Alert – Cisco Firewall Services Module (JSOC)

Green Tip of the Month

Say No to Paper or Plastic

You don't have to wait until grocery bags are banned: Say no to plastic or paper ones now. Instead, bring your own reusable shopping bags. Consider an entire set of reusable, double-handled hemp bags that work great for a large order, and reusable organic cotton mesh bags for your fruit and vegetables.

Remember: BYOB (Bring Your Own Bags).

The Daily Green

[redacted] News You Can Use

August 2009

Visit Our Website

Security Awareness Tips

DOD Urges Less Network Anonymity, More PKI Use. Black Hat 2009

LAS VEGAS -- The age of network anonymity may be coming to a close, according to a top defense official charged with cyber security. The United States needs to be more agile in defending against attacks from cybercriminals who are constantly infiltrating domestic networks, said Robert Lentz, CISO at the U.S. Department of Defense, during a keynote address to Black Hat USA 2009 attendees.

Lentz said the government continues its research into attack surfaces to produce an agile, dynamic defense capable of not only detecting but being able to take a proactive role to prevent future attacks against government infrastructure before they happen." It's all threaded in this area of driving anonymity out of network," Lentz said.

Contributing Source: Information Security Magazine Online

To view the latest JSOC Monthly Wrap-Up, visit our website at:
http://dojnet.doj.gov/jmd/irm/itsecurity/monthly-report.php

Computer User Tips

Social Networking Site Twitter Offline, Millions Frustrated and Lost.

The popular social networking site Twitter came under attack Thursday August 6, 2009 and was out of service for the better half of the day. Service was eventually restored by late that evening. The site was completely inaccessible for all of its users and analysts believe the denial-of-service attack may have originated in Russia or Georgia.

Social networking site *Facebook* and search engine giant *Google* fended off similar attacks on Thursday as well.

At about 10:30 a.m. E.S.T., millions of people worldwide received e-mail messages containing links to Twitter and other sites. When recipients clicked on the links, those sites were overwhelmed with requests to access their servers causing massive network traffic that created the denial of service.

Contributing Source: The New York Times Online

Spammers Exploiting Free File Storage on Websites

Automated account creation exploit lets spammers hide behind legitimate file storage services. An unusual attack technique has enabled spammers to distribute more than 1 million messages an hour using legitimate, free file storage services available on the Internet.

In a blog published earlier this week, AppRiver, a security services provider, describes the unusual approach. In a nutshell, spammers have created an automated method for creating accounts in popular free file storage services -- including *groups.yahoo.com*, *groups.google.com*, and *livejournal.com* - and are using those accounts to host their spam content. The use of these sites makes the spam appear to be legitimate, thus enabling it to bypass commonly used blacklists.

AppRiver has tweaked its own defenses to detect the new spam attack and block it, but traditional spam tools that blacklist IP addresses or domains will not block the new attacks.

Contributing Source: Dark Reading Online

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way - at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Using Caution with Email Attachments

Take the following steps to protect yourself and others in your address book:

- Be wary of unsolicited attachments, even from people you know
- Save and scan any attachments before opening them
- Turn off the option to automatically download attachments
- Consider additional security practices (i.e., firewall)

Contributing Source: US-CERT.gov

[redacted]

Security Advisory - Mozilla (JSOC)
Security Advisory - Java (JSOC)
Security Advisory - OSX (JSOC)
Top Ten Scams (JSOC)

Green Tip of the Month

Greening the Commute

American workers spend an average of 47 hours per year commuting through rush hour traffic. This adds up to 3.7 billion hours and 23 billion gallons of gas wasted in traffic each year.

We can ease this strain by carpooling, taking public transit, biking, walking, or a creative combination thereof.

Consider car alternatives, such as a hybrid or electric vehicle, motorcycle, scooter, or using a car sharing service, like Flexcar or Zipcar.

PlanetGreen

[redacted]

News You Can Use

July 2009

Visit Our Website

Security Awareness

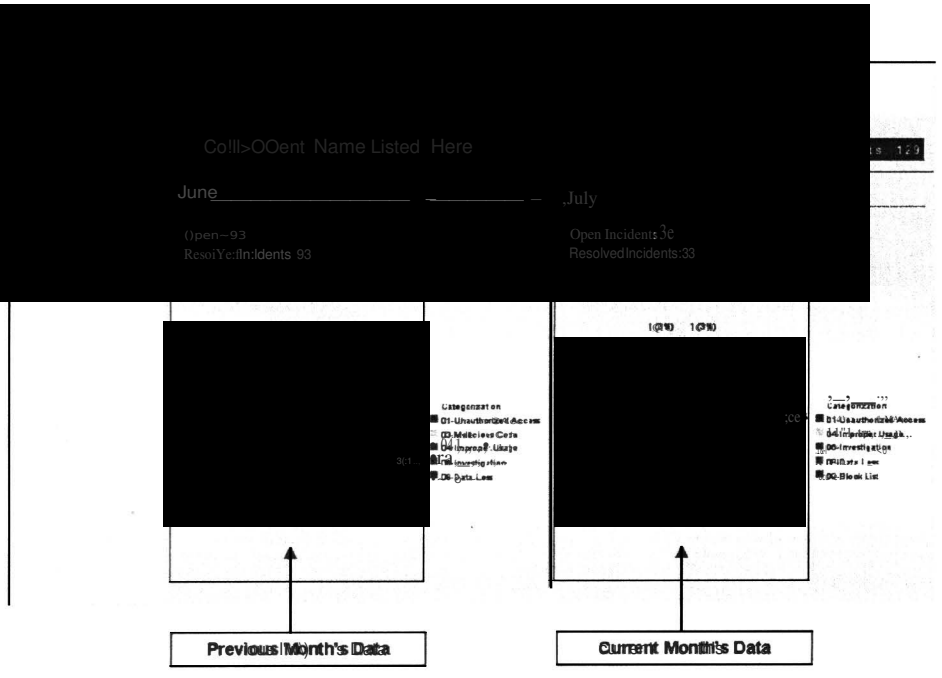
Incident Dashboards are now available to Components through JSOC's Remedy Web Portal

Component specific Incident Dashboards, available with a JSOC Remedy Web Portal account, provide Components with an easy to understand graphical view into their incident ticket status. The information displayed includes total incidents open, incidents reported by category from the previous month, and real-time open and closed incident ticket information by category for the current month.

The Incident Dashboard is accessible by clicking the dashboard button at the top of the JSOC's Remedy Web Portal's navigation bar.

For more information about your Component specific Incident Dashboard, contact Curtis W. Johnson at curtiswjohnson@usdoj.gov, or visit our website.

[redacted]



Computer User Tips

Guidelines to follow when publishing information on the internet

- **Be careful what you post to the internet.** Make sure you are comfortable with anyone seeing the information you put online, because people you don't know will find and share it with the people they know.
- **Realize that you can't take it back.** Once you post something online, it is available to other people and search engines. You can change or remove information after something has been posted, but it is possible that someone has already seen the original version.

Source: USCERT

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way - at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtiswjohnson@usdoj.gov.

Cyber Awareness Tip

640,000 New Fake Antivirus Variants

Researchers are expecting 640,000 new variants of the Fake Antivirus (Fake AV) malware in the third quarter of 2009. This increase is due to the ease at which Fake AV campaigns can be designed and distributed when compared to banking Trojan attacks which require professional programmers.

Source: Dark Reading

[redacted]

Critical MS ATL MS09-03 Patch, 7/30/09
(JSOC)

MS Critical Patches, July 2009
(JSOC)

Adobe Flash Patch, 07/23/09
(JSOC)

Oracle CPU Patch, 07/17/09
(JSOC)

Green Tip of the Month

Select 2-Sided Printing

The U.S. alone uses 4 million tons of copy paper annually, about 27 pounds per person, which accounts for 25% of all landfill waste.

Source: The Daily Green

News You Can Use

June 2009

Visit Our Website

Security Awareness Tips

JSOC's End of Month Report

The *JSOC Monthly Wrap-Up* provides an end of month summary of JSOC cyber threat activity highlights, VPR alerts, CTAT briefings, user awareness publications, and blocked domains, email addresses, and IP addresses. The report also contains an incident dashboard that breaks down incidents by category, provides further analysis of Malicious Code incidents (the Department's most identified threat category), and includes a list of the most popular internet hosts visited by Department users.

To view the latest JSOC Monthly Wrap-Up, visit our website at:
http://dojnet.doj.gov/jmd/irm/itsecurity/monthly-report.php

Computer User Tips

Cyber Criminals Roll Out Fake Microsoft Patch Malware Campaigns

Be on the look out for the following malware campaigns designed to emulate legitimate Microsoft (MS) updates. If you encounter any of these updates at work, record the URL and notify your IT Security staff as soon as possible. Home users should only accept MS program updates through Microsoft's website at www.microsoft.com.

- **Important Windows XP/Vista Security Update:** This fake update is often sent via email with a fake Conficker removal tool that can often be identified by Conficker being misspelled as "Conflicker".
- **Outlook Re-Configuration Campaign:** A fake Outlook Update executable file (outlook_update.exe) is being posted to legitimate websites that have been compromised. Outlook updates should only be performed through the MS website.
- **Critical Outlook Update:** This third malware attack should be familiar to most users as it's delivered via an email attachment (officexpKB890721-FullFileENU.exe). Do not double click attachments, especially .exe files, offering any type of software update.

Contributing Source: ZDNet

Adobe Implements Quarterly Security Patching Updates

Adobe released their first quarterly patch that addresses 13 critical PDF vulnerabilities to Reader and Acrobat 9, and earlier versions of this software. Adobe recommends users upgrade to the newly released 9.1.2 version as soon as possible. If you are running an older version of Acrobat or Reader, and can't upgrade, visit JSOC's Website for alternate version upgrades.

The Department's IT security staff performs software updates to your work computer, but check to make sure your home computer is set to perform automatic updates. If not, change this preference, or perform a manual update. Software that cannot be set to automatically perform updates should be updated manually on a monthly schedule.

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Twitter Users Targeted with First For-Profit Antivirus Scam

The first week of June introduced Twitter users to their first antivirus for-profit scam promising a "best video" via a fake YouTube website.

This is the same antivirus scam that has been circulating on other social networking sites and through email. The scam directs the user to a malicious site that installs the virus.

Contributing Source: The Register

MS Critical Patches, June 2009 (JSOC)

Choosing and Protecting Passwords (US-CERT)

Green Tip of the Month

Phantom Load

The EPA estimates consumers spend $100.00 a year on electricity used by electronics that are turned off or in stand by mode. EPA recommends:

- Unplug power adapters, battery chargers and other similar items.
- Use power strips so you can turn off electronics completely.
- Buy products that are highly rated by the federal Energy Star program.

The Daily Green

[redacted] News You Can Use

May 2009

Visit Our Website

Security Awareness Tips

Internet Surfing Dangers

[redacted] Cyber attacks originating from unsafe websites and email are becoming increasingly sophisticated and focused on everyday communication channels as more and more revenue is acquired. Malicious coders are designing their websites to be exact replicas of legitimate websites, and then advertising these sites via web ads and Internet searches. Fake search engines and misspelled website domain traffic are big business, especially in the financial and social networking market, because visitors think they are on a real website and share their information without suspicion. Users are at serious risk of encountering one of these phony websites if they spend time surfing and sharing information over the Internet.

The Department will begin implementing BlueCoat™ filters in accordance with DOJ order 2740.1A to help protect its networks against existing threats and non-work related Internet usage. Non-work related Internet usage continues to be one of the largest threats to the Department's information security. Remember, network security is everyone's responsibility.

New Information Phishing Schemes

Fake information gathering schemes based on popular topics, themes, and games are being created by identity thieves to entice users into entering personal information. These types of groups or discussions often require the user to input their first pet's name, mother's maiden name, street address, first school, etc. to join/register before the user can participate.

Disclosing of this kind of personal identifying information is very useful to identity thieves as it's the same type of information required by web email accounts, legitimate websites, and banking institutions. Be careful with any personal information as it is very difficult and expensive to rebuild a "digital identity" once it has been compromised.

If you encounter this kind of request for personal information at work, do not fill in the information; note the URL, and report it to your IT security staff as soon as possible. Information solicitations received at home can be ignored by closing the browser window or navigating to a new website.

Computer User Tips

Update and Patch Your System Software Often

As soon as a security patch is announced, malicious coders are hard at work writing code into their websites and email attacks to exploit information from your computer, before they can be patched. Coders have reduced the time it takes them to write code to exploit a new vulnerability from weeks or days to hours! Microsoft automatic updates are performed every Tuesday in what is referred to as "Patch Tuesday". The Department's IT security staff performs these updates to your work computer, but check to make your home computer is set to perform automatic Microsoft updates. If not, change this preference, or perform a manual update. Software that cannot be set to automatically perform updates should be updated manually on a monthly schedule.

What is the JSOC Newsletter?

The Justice Security Operations Center **News You Can Use Newsletter** keeps our readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any issues, subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Social networking sites are delivering malware 10 times more effectively than email.

Kaspersky Labs's *Malware Evolution 2008* report indicates that 10% of all malware delivered via social networking sites are successfully installed onto members' computers.

Kaspersky Lab collected over 43,000 malware samples from social networking sites in 2008, while McAfee reported 800 new variants of the Koobface virus.

Contributing Source: eWeek

[redacted]

JSOC Fake Antivirus Information (DOJ)

Why is Cyber Security a Problem? (US-CERT)

Green Tip of the Month

Junk Mail

Each year millions of trees and billions of gallons of water are used to create junk mail. To be removed from the national mailing lists -- send your name, address, and signature to:

Mail Preference Service
c/o Direct Marketing Association
P.O. Box 643, Carmel, NY 10512

Source: *nationalzoo.si.edu*

News You Can Use

April 2009

Click Here To Visit Our Website

Security Awareness Tips

Conficker Worm

The new version of Conficker, identified on April 9, 2009, attempts to install new malicious code, scareware, and Waledac / Downadup onto infected computers. This new version is especially dangerous as these software additions are designed to scare and trick users into navigating to malicious websites that capture personal and financial information.

If you believe your home computer may be infected with Conficker, there's an easy way to find out. Conficker blocks access to websites that contain software that may interfere, block, or remove its installation. Open your internet browser at home and try to visit the following websites: www.microsoft.com, www.mcafee.com or www.symantec.com. If you are unable to reach these websites, your computer may be infected. Please click here to read USCERT's information on how to detect / remove Conficker from your home computer.

Contributing Sources: USCERT, CNet, Washington Post

Malicious Email (Spam)

Spam accounts for over 97% of all email, and is still a main delivery vehicle for malicious coders who propagate their malware, botnets, and viruses over the internet. While there have been successful shutdowns of spam sending companies (McColo's closure in Nov. 2008 resulted in a 60-70% reduction in malicious mail and botnet delivery in the US during Nov. and Dec. 2008), there are others that have stepped in and already increased spam delivery rates above pre-McColo levels.

- **Fake Conficker Infection Alerts**
  Scareware email campaigns are circulating that try to scare the recipient into accepting fake antivirus software by saying the recipient's computer is infected with Conficker. If infected, the computer will attempt to download the Waledac botnet and spread the virus to other computers.
- **Stimulus Package Offers**
  Malicious email is circulating with the IRS logo and pictures of President Obama that advertise available stimulus package money for cash strapped individuals. These emails request personal, credit card, and other financial information to verify that the recipient is qualified for stimulus funds.
- **Tax Return Solicitation**
  Fake tax return emails are being sent that offer "cash now" in exchange for the recipient's tax return, or charges for services to expedite a tax return. These emails are designed to collect your Social Security number, date of birth, mother's maiden name, credit card information and the PIN for your ATM card. ***Tip: The IRS never initiates contact with taxpayers via e-mail if it has to do with your account or private information.***

Be very suspicious of any emails you receive from strangers, companies, or government agencies that request personal, financial, or credit card information. If you receive an email that directs you to a website requesting you to download or update a program, do not accept the offer and close the web browser window. Click here for instructions on how to report any malicious / spam email you have received at work to your IT security staff or JSOC.

Contributing Sources: SecurityFocus, SecurityPark, CNet, ZDNet, MSN

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps our readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any issues, subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

JSOC'S NEW WEBPAGE ONLINE

JSOC's new webpage on DOJNet contains all its cyber security alerts; cyber briefings, user awareness papers, and newsletters. Please click here to visit JSOC's webpage.

- Incident Report Form
- Malicious Email Submittal
- Incident Response Plan (IRP) Information
- Critical Vulnerability Alerts
- Vulnerability Alerts
- Cyber Threat Advisories
- White Papers
- News You Can Use Newsletter
- CTAT Cyber Daily Briefing

Microsoft Releases 5 Critical Updates on April 14, 2009
(Microsoft)

Green Tip of the Month

Turn Off Your Gaming Console.

A gaming console that is left on twenty four hours a day, seven days a week, will use as much electricity annually as two new refrigerators.

(Green Living Tips)

[redacted]

News You Can Use

March 2009

Click Here To Visit Our Website

Security Awareness Tips

Social Networking Websites and Job Boards

[redacted]

There continues to be a surge in malware, viruses, and botnets directed toward and residing on social networking and job board websites. Malicious coders have turned their attention to these websites (See USAJobs Advisory) because of the wealth of information available, and the relative ease at which members seem willing to share it.

If you are a member of a social networking or job board website, change your password today, and change it often. Use a password that is at least 8 characters long with a combination of upper and lower case letters, numbers, and special characters.

Malicious Web Sites Encrypt Local Files

A rush of new fake antivirus websites are being designed to emulate authentic sites due to the success they have had at tricking visitors into downloading their malicious content. Some of these websites contain "scareware" programs that attempt to scare the visitor into installing their malware or virus. These websites are normally identified by warning messages or pop-ups that tell the visitor a software upgrade is needed or something bad is happening to the visitor's computer, and offers their software as the solution. Unfortunately this action results in installing the malware or virus the visitor was trying to avoid.

A few scareware sites have introduced a new feature into their malware – encryption. **This new version attempts to encrypt and scramble files inside the visitor's "my documents" folder when installed**. Once the encryption process is complete, the visitor must purchase an encryption key from the malicious site to access their files.

If you visit a website you think is malicious, please report it to your IT security staff as soon as possible.

Contributing Source: Washington Post

Computer User Tips

Website Passwords

Two-thirds of computer users use one or two passwords to access all their websites. If you are one of these users, do not allow your web browser to automatically save your passwords. This practice allows anyone with physical or remote access to your computer, access to your web site accounts. If your browser supports an encrypted master password, your saved passwords may be more secure, but there are programs designed to break this encryption.

Contributing Source: NY Times

Secure Your Wireless Router at Home

When installing a wireless network at home please take the proper steps to ensure it is secure. Look in the manual for how to change the wireless ID (also known as the SSID) to something unique. Turn on the Wi-Fi Protect Access (WPA or WPA2) for authentication, enable Temporal Key Integrity Protocol (TKIP) for encryption, and use Media Access Control (MAC) address filtering. An unsecured wireless network allows other computer users to use your bandwidth for free, and possibly use it for illegal activities. If the police come looking, a person with an unsecured network would have a difficult time proving the activity didn't come from one of their computers.

Contributing Source: SANS

What is the JSOC Newsletter?

The Justice Security Operations Center **News You Can Use Newsletter** keeps our readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Fake Waledac Coupon Websites

Couponizer.com, a legitimate site used to optimize and gather coupons, is the latest target of the Waledac virus. Fake Couponizer websites are now online that utilize IP geolocation databases to locate website visitors. This solution is new for Waledac websites, and allows coders to further trick the visitor by offering national and local coupons based on the visitor's location.

The Waledac virus, which infects computer systems to collect email addresses, is delivered as an email or Ecard that directs the recipient to a fake website that installs the virus when clicked by the visitor.

[redacted]

USAJobs Cyber Threat Advisory (JSOC)

Adobe Acrobat and Reader Vulnerability (JSOC)

Green Tip of the Month

Public Transportation

A person riding public transportation can achieve an average annual savings of $8,481, based on today's gas prices and average parking costs.

(APTA)

News You Can Use

February 2009

Click Here To Visit Our Website

Security Awareness Tips

Cyber Crime in 2009

Data capture, passwords, and account numbers will continue to be the target of malicious coders in 2009. While the Department of Justice is utilizing all resources to protect its users against these risks, home users are expected to encounter a dramatic increase in fake email and malicious websites. Industry also predicts mobile cell phone networks are the next target due to the advances, popularity, and the variety of ways smart phones are being used.

- **Data Capture:** Malicious coders are constantly modifying the schemes they use to gather information from unsuspecting users. Be careful when opening email attachments, accepting free offers, and surfing the internet. There is someone out there trying to collect your information.
- **Smart Phones:** Voice and touchtone phishing (much like email and web phishing), malware, and cellular botnets are predicted to become a serious threat to the mobile network in 2009. Malicious code is being written to take advantage of the growing trend in mobile interactivity with companies that require social security numbers, account numbers, and passwords to verify identity. High value targets will also include individuals that interact with financial institutions to transfer funds and stocks through mobile devices.

Contributing Source: Emerging Cyber Threats Report 2009, Georgia Tech Information Security Center

Social Networking Risks

Social networking is often used to find old friends, create new friends, and network with people of common interest. This free exchange of information establishes a false sense of security as the user thinks only "friends" are viewing their posted information. Malicious coders exploit this vulnerability by inviting contacts within the network to click on their page. Once clicked, the embedded code infects the visiting user's computer and directs it to collect personal information from the user, the user's friends, and user's groups on the network.

Fake Antivirus Software Updates Wreak Havoc across the Internet

Malicious software disguised as a legitimate Antivirus Update is tricking users into downloading and installing its Trojan virus. Recently, there has been a significant increase in Fake Antivirus (AV) Trojan Horse software that is utilizing social engineering principles to fool unsuspecting users into compromising their own machines. Do not upgrade your antivirus software through hyperlinks offered by unknown website or pop up windows. These software updates are automatically provided by the DOJ IT service providers at work. If you believe your antivirus software at home needs an update, open the program from your desktop and select the button or link provided to perform a manual or live update. (*JSOC White Paper*)

Computer User Tip

A Trick for Remembering Long Passwords

When creating a password, users should avoid common words, proper names, and randomly generated passwords such as "GrTlkOPk6SS!", which would be impossible to remember. Try using a phrase that is familiar and easy to remember (example: "IBowledA2855!"). This password meets the Department's 12 character password requirements by using uppercase and lowercase letters, numbers, and symbols.

Contributing Source: SANS

What is the JSOC Newsletter?

The Justice Security Operations Center **News You Can Use Newsletter** keeps our readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect against cyber threats on the Internet.

These threats affect you everyday in every way – at the office, at home, and in between. This is information you need to know, written in terms you can understand.

If you have any issues, subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Threat Tip

Fake Greeting Card emails are distributed to capture data and email addresses.

Internet scams, charity fraud, fake websites, and unsolicited e-mail will intensify around the Valentine holiday. Exercise caution when visiting new websites or opening email offering free items, gifts, e-cards.

Malware writers and spammers are designing increasingly convincing email and fake websites to fool visitors into accepting their viruses.

[redacted]

Defending Cell Phones and PDAs Against Attack (US-CERT)

Green Tip of the Month

Donate or Recycle Old Cell Phones

Cell phone upgrades cause consumers to throw away over 130 million working cell phones each year.

News You Can Use

December 2008

Visit Our Website

Security Awareness Tips

Malware Targets USB and Removable Media

In recent months, JSOC has identified a significant rise in the number of dangerous malware downloads targeting removable media devices. This rise has been attributed to malicious coders writing malware focused on infecting USB and removable media storage devices to spread the virus quickly.

Thumb drives, external hard drives, CD/DVD-RW, and flash media (digital camera/phones) are targeted because they are portable, and easily exchange information between computers. When infected devices are connected to a computer they attempt to install Trojan software that runs in the background unnoticed by the user.

Steps you can take to help protect your home pc:

- **Disable Auto-Run.** It's important to disable Auto-Run as this feature allows removable media to automatically start or install any software programmed to run when the device is inserted into a computer. This allows the Trojan to spread throughout your computer and connected devices. Please see the help instructions on your home computer to disable Auto-Run.
- **Install Firewall and Antivirus Software.** Windows XP and VISTA come with a firewall that protects against most intrusions, please make sure it's enabled and updated on a weekly basis. Norton and MacAfee, along with many others, also offer "off the shelf" choices for both firewall and antivirus protection solutions.
- **Create a User Level Login** *(without administrative privileges),* and use it as your main login account. This helps reduce your risk of infection, and denies full administrative access to your computer in the event your login credentials are compromised. ***An Administrative Login should never be used when connecting to the internet.***

Computer User Tips

Avoid Malicious Code and Software

Current web technology makes it possible to embed additional code inside a primary webpage. Hackers are able to misuse this technology to carry out malicious activities, such as redirecting the user's web browser to websites that secretly download intrusive software. A number of popular websites have been impacted by these attacks because the code is sophisticated and hidden from plain view.

Steps you can take to help protect your home pc:

- **Upgrade to Microsoft's Internet Explorer 7.0 (IE 7).** IE7 includes many user friendly enhancements and new security features that help protect against malware intrusions.
- **Regularly Update Computers and Applications.** Ensure Microsoft Update is scheduled to check weekly for product updates. Applications that do not automatically perform weekly updates should be updated manually.
- **Improve Your Password Security.** Increase your password length to a minimum of 12 characters that include upper and lower case letters, and at least one number and special character. A longer password provides significantly higher protection from unauthorized access.

Questions regarding this newsletter, or requests for permission to redistribute should be directed to:

JSOC/DOJCERT 202-307-5332

What is the JSOC Newsletter?

The Justice Security Operations Center ***News You Can Use Newsletter*** keeps our readers up to date on the latest topics, security vulnerabilities, and computer user tips to help protect them against cyber threats on the Internet.

These threats can affect you everyday in every way – at the office, at home, and in between. This is information you need to know, in terms you can understand.

If you have any issues, subjects, or ideas you would like to see addressed in future newsletters, please email Curtis Johnson at curtis.w.johnson@usdoj.gov.

Cyber Awareness Tip

Facebook's users are targeted by a virus named "Koobface".

This virus spreads via a note from a friend that might say, *"You're really funny in this video."* If clicked, the link connects to a website which asks you to download an update to your Adobe Systems Flash player. This link will attempt to install the Koobface on your computer.

Koobface modifies user profiles to redirect their visitors to malicious websites.

[redacted]

DOJ Cyber Security Conference (DOJ)

Dealing with Cyberbullies (US-CERT)

Obama, McCain Lessons in Cyber Security (Security Focus)

Green Tip of the Month

Recycle Your Fluorescent Bulbs

The Mercury from one fluorescent bulb can pollute 6,000 gallons of water beyond safe drinking levels.