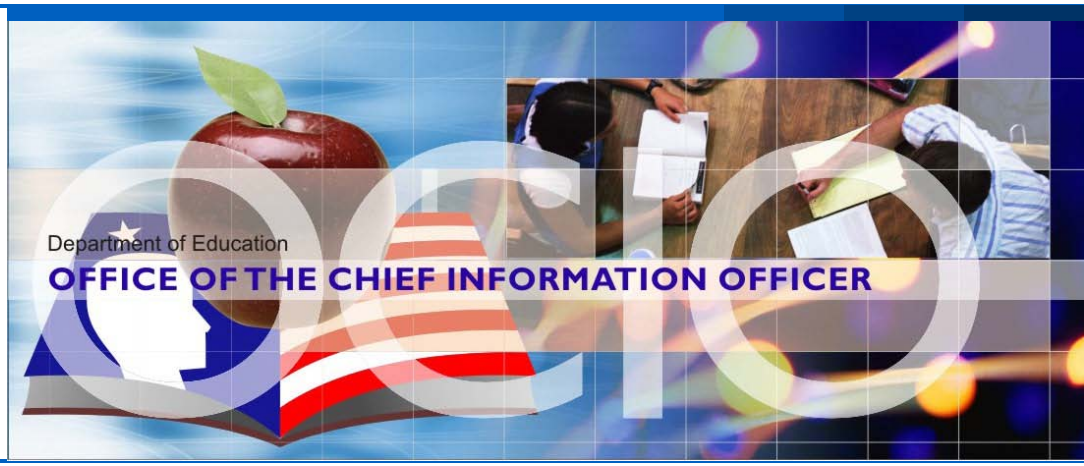
Department of Education
Office of the Chief Information Officer

U.S.Department of Education

Office of the Chief Information Officer



Beyond Threats: Working with IT Security Professionals

For Official Use Only

Eric Eskelsen
Office Chief Information Officer,
US Department of Education

Purpose

- **To inform about and understand current security threats**
- **To establish and framework discussions with IT Security professionals**

Emerging Cyber Doctrine

" In the near future, information warfare will control the form and future of war... Our sights must not be fixed on the fire-power of the industrial age; rather, they must be trained on the information warfare of the information age. "

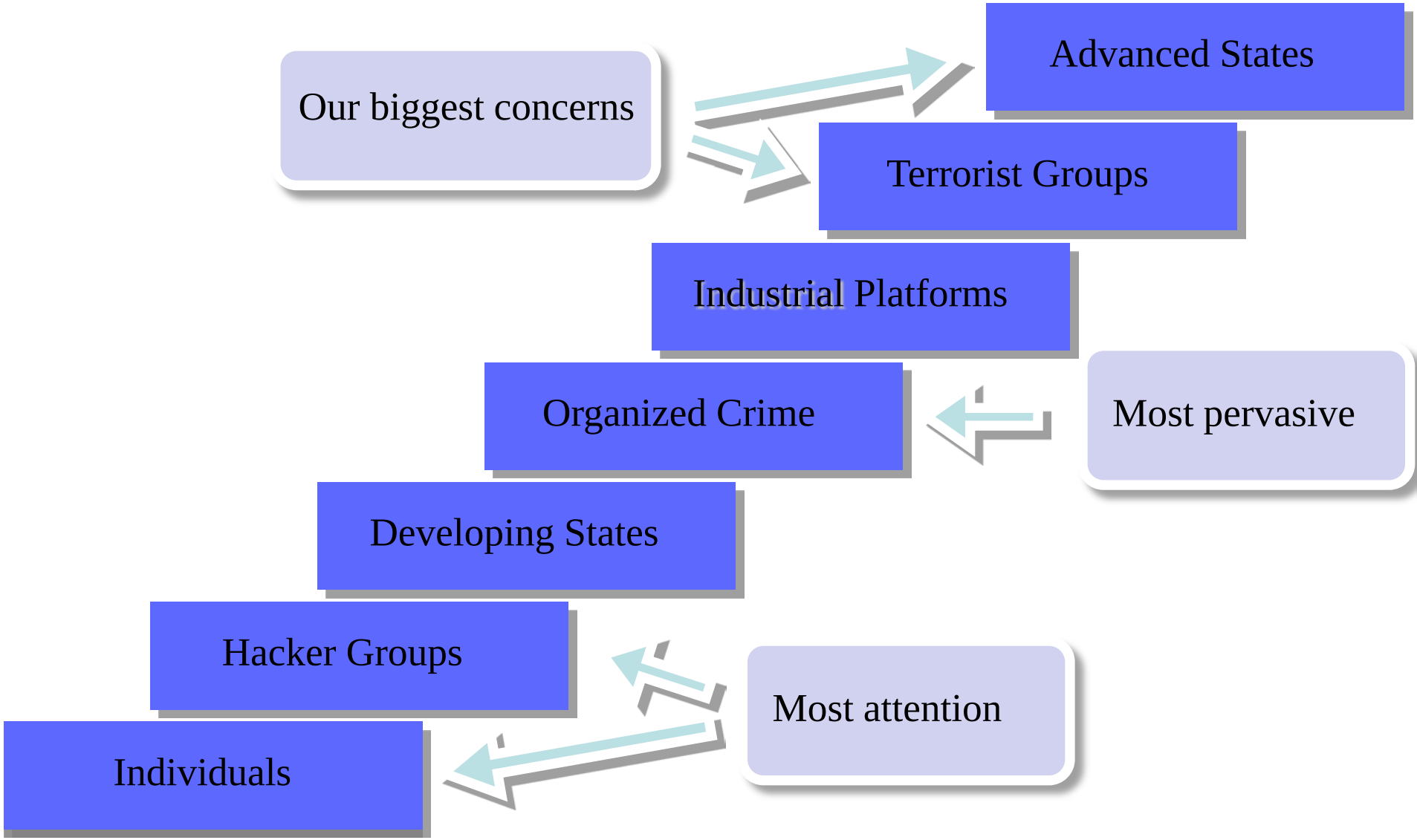
-- Major General Wang Pufeng
Peoples Liberation Army, China

What's New and So What

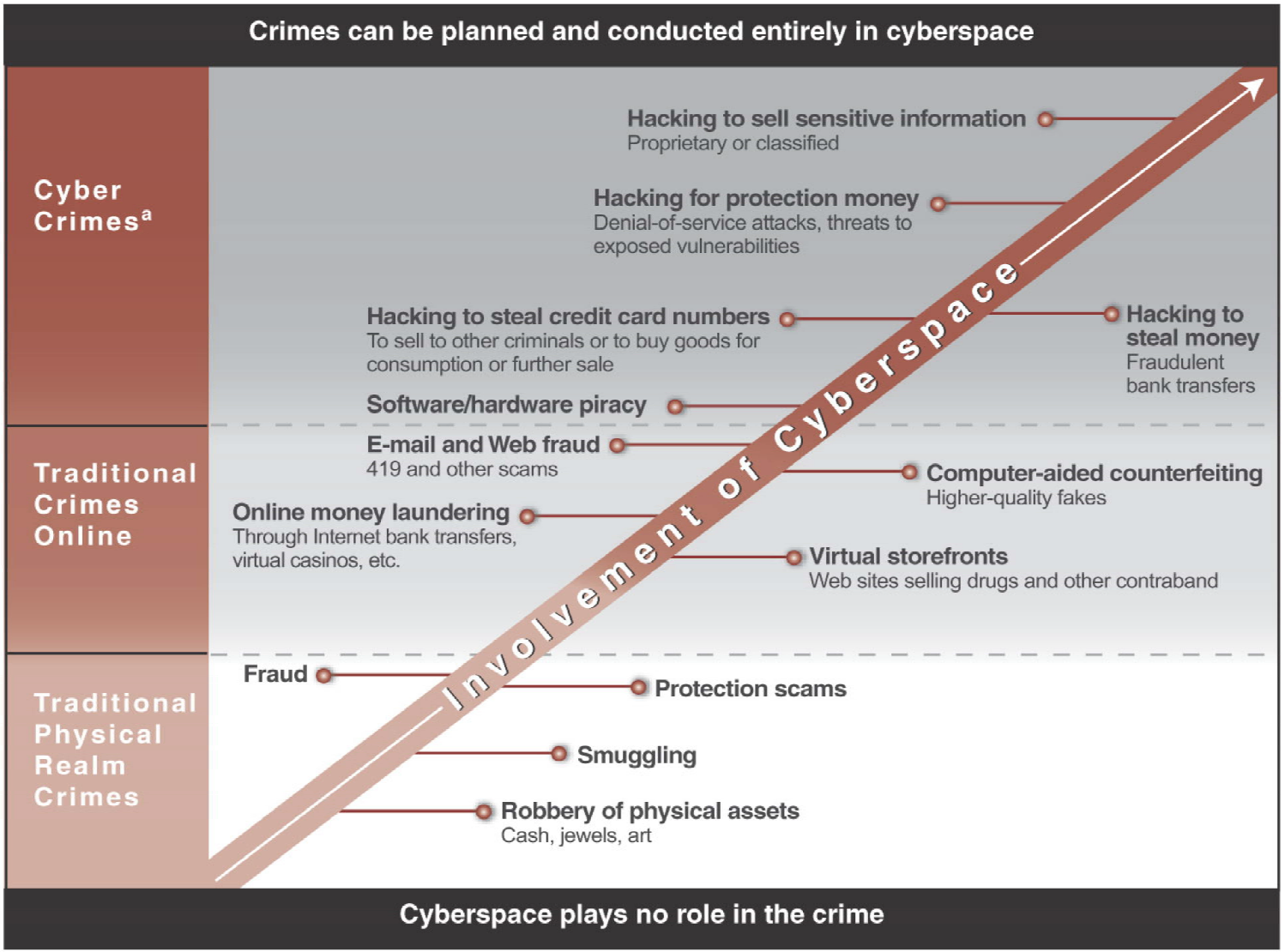
The reconnaissance phase of a Cyber war is already taking place -- we are already under attack !!

- **High interest in all cabinet personnel and travel OCONUS**
- **Intel Agencies seek Political, Economic and military**
- **All mobile devices are targets**

Known Threat Actors



Spectrum of Cyber Crime



[a] *Cyber crimes can be conducted entirely online.*

Examples

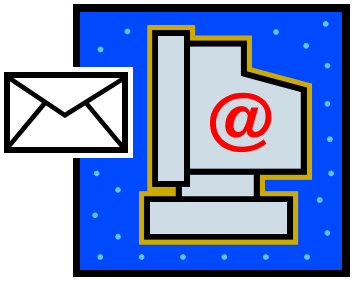
- **Exfiltration of US sensitive data from local networks and systems committed by hostile Nation States increasing.**
- **FBI Report to Congress: Al-Qaeda terrorist cell in Madrid used stolen PII/ SI to conduct much of their business.**
- **Increased cases of a critical nature against critical networks identified by the US-CERT**
- **In FY 2009, events detected will continue to rise**
- **Stronger awareness and countermeasures will be required to protect against future threats.**
- **Monster.com is advising its users to change their passwords after data including e-mail addresses, names and phone numbers were stolen from its database. *January 26, 2009***
- **Nearly nine in 10 corporate data breaches could have been prevented had reasonable security measures been in place - *Verizon Forensic Investigations***
- **USDA, unknown hackers may have illegally accessed a USDA database containing PII information - approximately 26,000 Washington, D.C., area employees are potentially at risk for identity theft.**
- **DOT OIG, lost over 100,000 state of Florida Drivers PII.**

Identity Theft - Top Risks for all Users

A data breach disclosed by Heartland Payment Systems may well displace TJX Companies' January 2007 breach in the record books as the largest ever involving payment data with potentially over 100 million cards being compromised. *January 26, 2009*

Classical phishing attack – Top Risks for all Users

Sends email: “There is a problem with your eBuy account”



Password sent to bad guy

User clicks on email link to www.ebuj.com.

User thinks it is ebuy.com, enters eBuy username and password.

Phishing Example

Home > Shows > Daily Debrief > Daily Debrief Blogs

THE DAILY DEBRIEF

Monday-Friday, 3-7pm
with Chris Dorobek and Amy Morris.

Sponsored by THE FRED FEDERAL SHOW

Phishing Scams and Your TSP

January 26, 2009 - 4:08pm

Phishing Scams and Your TSP
Tom Trabucco, TSP
Play Download mp3

An online phishing scam for Thrift Savings Plan passwords is targeting a group of federal employees.
Officials at the TSP are attacking the problem.

Print Email A- A+

Tom Trabucco is Director of External Affairs and tells us what happened.

Financial Exploits - Top Risks for all Users

A data breach disclosed by Heartland Payment Systems may well displace TJX Companies' January 2007 breach in the record books as the largest ever involving payment data with potentially over 100 million cards being compromised. *January 26, 2009*

COMPUTERWORLD Security — IDG

JUMP TO More Resources — SEARCH Google™ Custom Search GO

- Home
- News
- E-mail Newsletters
- + Blogs
- + Shark Bait
- − Knowledge Centers
  - + Operating Systems
  - + Networking & Internet
  - + Mobile & Wireless
  - − Security
    - Cybercrime & Hacking
    - Spam, Malware & Vulnerabilities
    - Security Hardware & Software
    - Standards & Legal Issues
    - Privacy
    - Intellectual Property & DRM
    - Disaster Recovery
  - + Storage
  - + Business Intelligence
  - + Servers & Data Center
  - + Hardware
  - + Software
  - + Development
  - + Careers
  - + Management
  - + Government
- − Opinion
  - Columnists
  - SharkTank
- Webcasts
- Video
- Podcasts
- White Papers

Data breach at Heartland may be bigger than TJX's

By Jaikumar Vijayan — Comments 1 — Recommended 8 — Share

January 26, 2009 (Computerworld) A data breach disclosed last week by Heartland Payment Systems Inc. may displace the one revealed by The TJX Companies Inc. in January 2007 as the largest compromise of payment card information to date.

Heartland, a Princeton, N.J.-based payment processor, said intruders broke into its systems sometime last year and planted malware that they used to steal credit and debit card data.

A Heartland spokesman said Thursday that the company still had no idea how many cards had been compromised. It wasn't even sure how long the malware had been on its network, he noted. "All we know is that it was there for a period of time in the second half of 2008," he said.

But given that Heartland processes more than 100 million card transactions per month, it's conceivable that the number of compromised cards could be at least that high, said Gartner Inc. analyst Avivah Litan. In the TJX breach, 45.6 million card numbers were stolen over 18 months.

"Everybody who processes card information is dying to know how exactly this happened," said Henry Helgeson, president and co-CEO of payment processor Merchant Warehouse Inc. "One of our frustrations right now is, if this is a new attack, we need to know about it."

The Heartland breach was the second disclosed by a large payment processor in recent weeks. On Dec. 23, RBS

Top Stories | Related

- Microsoft delivers IE8 release candidate
- Update: Sprint to lay off 8,000 by April
- EU may demand Microsoft bundle rival browsers with Windows
- Future Watch: A.I. comes of age
- Food poisoning outbreaks could prove a boon to RFID
- Microsoft extends Windows 7 beta download deadline

RESOURCE ALERTS

SIGN-UP to receive Security Resource Alerts

Webcasts

How to Future-proof for Mobility: An Integrated Management and Security Strategy

Preparing for PCI 1.2 Web Seminar

Winning Enterprise Authentication: 5 Key Steps for Success

Whitepapers

A Practical Guide to Building An Effective Patch Management Process

Best Practices for Building a Sustainable PCI Compliance Program

Not all QSAs are Created Equal: What You Need to Know Before you Buy

Computerworld Reports

Trend Micro Gets Smart with a Hybrid Approach

Computerworld Technology Briefing: Intelligent Users Use Business Intelligence

Trend Micro Gets Smart with a Hybrid Approach

Keyloggers - Top Risks for all Users

Keylogger (or Keystroke Logger): Tracking Software or Hardware that records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the Keylogger.

Home > Articles > Keyloggers, trojans net hackers "several hundred dollars a day"

Posted : Jan 5, 2009 | By: Marcia Savage

Keyloggers, trojans net hackers "several hundred dollars a day"

Tools: Print article | Email a friend | RSS Feeds

A recent study of keyloggers and banking Trojans provides a view into the underground economy of stolen bank account credentials, passwords and credit card numbers.

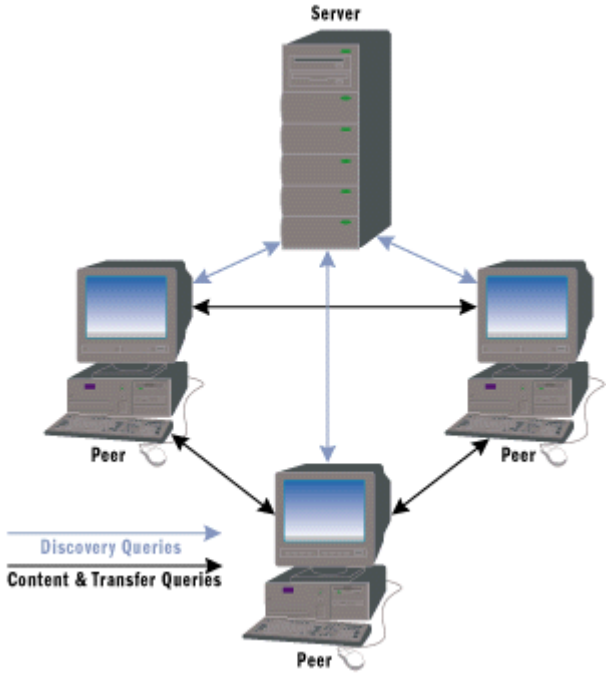
The study, published earlier this month by Thorsten Holz, Markus Engelberth and Felix Freiling at the University of Mannheim in Germany, analysed malware designed to steal sensitive information from infected machines. The researchers developed techniques for studying the "dropzones" -- servers that are used by attackers to store stolen information.

Over a seven-month period, they were able to access more than 70 unique dropzones and found about 33GB of stolen data from more than 170,000 compromised machines. Among the stolen data, the researchers found more than 10,700 stolen online bank account credentials, about 149,000 stolen email passwords, and 5,600 full credit card details.

Peer 2 Peer File Sharing – Top Risks for all Users

US DOT Chief Privacy Officer (CPO) released government DOT and National Archive documents onto P2P File Sharing Network

- CPO's daughter installed PEP software on home computer
- Computer contained DOT and National Archive
- Documents found by Fox News Reporter using Limewire



Wireless In-Security - Top Risks for all Users

The Register®
Biting the hand that feeds IT

Hardware Software Music & Media Networks Security Public Sector Business Science
Crime Enterprise Security Anti-Virus Spam ID Spyware

Print story Post comment Track this topic

TJX closes book on infamous security breach with sale

Everything must go

By John Leyden • Get more from this author

Posted in Crime, 23rd January 2009 16:19 GMT

VMware whitepaper - The business case for Virtualization

TJX, the discount retailer that was the target of one of the largest information security breaches on record, rewarded customers with a a special sale offering 15 per cent discounts in all its US and Canadian stores on Thursday.

The one-day "Customer Appreciation" sale was billed as the firm's way of expressing its appreciation for customers for retaining their loyalty after it did such a bad job of retaining their records. Two years ago TJX suffered a long-running security breach, later traced as starting off from an insecure wireless network as one of its stores, which resulted in the exposure of 45.7m credit card records, going by conservative estimates. Other estimates put the figure at 94m accounts.

"insecure wireless network"

For Official Use Only

USB Drives / Mobile Media - Top Risks for all Users

An infected USB drive can spread its payload to any computer that it is connected to in the future

Hackers will use USB devices to launch attacks

USB memory keys 'pose virus risk'

Criminals are using USB keys to infect people's PCs, according to security company

Written by Dinah Greek, Computeractive

20 Jan 2009

"Conficker Virus"

Attacks on PCs will increasingly be launched from infected USB keys and other solid-state memory devices, according to makers of computer security software.

The ease with which hackers can harness such devices, used in cameras, picture frames, and other consumer electronics, to infect PCs has been highlighted by **F-Secure** and **McAfee**.

One example found this month by F-Secure shows how fraudsters are using the autorun.inf files to spread the Downadup worm via flash memory devices. In the install and run category, the worm replicates the open folder action in order to install itself.

USB Drives / Mobile Media - Top Risks for all Users

New Zealand Man Buys Thrift-Shop MP3 Player Full of US Army Classified Information

Posted by John Mahoney at 3:30 AM on January 27, 2009

An MP3 player purchased for $US14.50 (brown Zune?) at an Oklahoma second-hand store had an extra surprise inside--60 files containing Iraq- and Afghanistan-deployed soldiers' personal info, a mission briefing and base equipment manifests. Score!

Chris Ogle, who hails from the Kiwi town Whangerei, says the device (sadly unspecified) never worked as an MP3 player, and when he plugged it in to diagnose why, said military files were found. Included in the dump are large lists of deployed soldiers with their SSNs, mobile phone numbers and health info, as well as lists of equipment deployed to various bases and mission details.

Why the Increase In Cyber Intelligence

- **Recent open source network compromises disclosure, becoming more common, used as a nation enabler**
- **Easier to steal digits, than to integrate a spy**
- **Larger ROI in stealing R&D, vice actually doing it. (Past events have shown that .EDU has been used as a gateway to .GOV)**
- **Economic motivation**
- **Globalization empowerment**
- **Continuous national interest into US directions and intentions**
- **If you can't out shoot them out spend them. (costly to recovery from breaches)**

Good Security Habits

- **Regularly install new Microsoft security patches**
- **Use anti-virus software**
- **Install spyware blocking software**
- **Install spam blocking software**
- **Change password(s) - Make them strong, and change them often.**
- **Disable auto-download or auto-open features**
- **Turn off file and printer sharing**
- **Install a hardware firewall**
- **Backup, backup, backup - Do it early and often.**

Why does it matter?

- **Security professionals must ensure that threats are remediated**
- **Security professionals must ensure organizational policies are upheld**
- **Security is everyone’s responsibility**