





SA J. Medeiros
Memphis Division
Cyber Crime Squad
615-232-7549
j.medeiros@ic.fbi.gov

The image is a dark blue rectangular box. At the top center is the official seal of the Federal Bureau of Investigation, which is circular and features an eagle, a shield, and the words 'DEPARTMENT OF JUSTICE' and 'FEDERAL BUREAU OF INVESTIGATION'. Below the seal, the name and contact information for SA J. Medeiros are listed in a bold, yellow, sans-serif font.

Internet Issues
???

- Technology is affordable, smaller and more powerful.
- Technology is easy to use.
- Who isn't on the Internet?
- Every aspect of our lives is dependent on the Internet
- High speed access is available to the masses (United States and around the world) World is going wireless.
- It's inexpensive.
- Less risky than traditional crime.
- The Internet has no boundaries. Increase in cases originating from the former Soviet Union, Africa and the Far East. Lack of international Cyber laws.
- All the tools you need to commit crimes are available online.

The image is a dark blue rectangular box. At the top center, the text 'Internet Issues' is written in a bold, yellow, sans-serif font, followed by '???' in a smaller, italicized, yellow, sans-serif font. Below this, a list of seven bullet points is presented in a yellow, sans-serif font. Each bullet point is preceded by a small yellow dot.

Threats

- **Poisoned pages**
- **Trojans**
- **Socialing**
- **Password attacks**

MySpace Hijacking

- MySpace pages are basically HTML
- Create a “poison” page to trap visitors/friends
- Use trapped information to login
- Deface/alter the pages of others
- Send “SPAM” Bulletins (messages)
- Insert code that “trojanizes”
- Nearly the same process works on Facebook

Facebook Worm

- “My Ex-Girlfriend Cheated on me...Here is my revenge!”
- Uses creative CSS and an iFrame
- Initiates a “share event” on every click

Drive-by Trojans

- **Troj/JSRedir-AK** is a variant of the JSRedir family that has had a massive impact since early December 2009. JSRedir infections are unintended JavaScript code that is embedded in a website to silently redirect surfers to malicious content on other websites. This is known as a drive-by download.
- For the month of January 2010 this infection made up more than [40 percent of web detections discovered by SophosLabs](#) dwarfing other web infections in prominence.

Trojans

- Malicious code concealed in useful program
- May allow “snapshots” of data
- May allow file exporting
- May allow keystroke recording
- May allow remote control of system

Imbedded Trojans

- **Energizer DUO USB Battery Charger Software Allows Remote System Access**
- *added March 8, 2010 at 10:26 am*
US-CERT is aware of a backdoor in the software for the Energizer DUO USB battery charger. This backdoor may allow a remote attacker to list directories, send and receive files, and execute programs on an affected system. The software, which has been discontinued, was available for both Windows and Apple Mac OS X versions. Only the Windows version is affected by this vulnerability.

Adobe

- For 2009, 80% of all exploits utilized malicious Reader documents

Tweets

- 140 character messages
- Tiny URLs, <http://tinyurl.com/2unsh>
- May not direct user to desired content
- Masks attack HTML page, or copycat page

Peer to Peer file sharing

- Makes a direct connection between two computers
- Chat is possible in most clients
- Rife with viruses and trojans
- Mostly unregulated
- Most traded are infringing videos, music

Social Engineering

- Pretending to be someone you are not in order to get someone to provide information or take an action they otherwise would not.
- Normally done by telephone.
- E-mail and chat are also being used.
- Being combined with Spear-phishing for maximum believability.

Telephones

- Vishing – Use of VOIP to establish presence.
- Caller ID Spoofing

Password Reset Attack

- Most sites allow users to store answers to select questions in order to gain access to the account and reset the “forgotten” password.
- Only works if the answers are truly only known to you.
- Gives access to E-mail, Social Networks, etc.



SA J. Medeiros
Memphis Division
Cyber Crime Squad
615-232-7549
j.medeiros@ic.fbi.gov
