VOLUME III, ISSUE I

SECURITY AWARENESS NEWSLETTER

FEBRUARY 2006

Published by: COT, Division of Communications, Security Administration Branch

INSIDE THIS ISSUE:

SECURITY TIP

Use "anti-virus software" and keep it up to date. Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. Be sure to update your anti-virus software regularly!

PREDATORS IN THE WILD

Editorial by: Robin Proctor

You may have seen the recent programming airing on NBC concerning Online Predators. I have to admit these days not much shocks or surprises me. However, I can still be repulsed and appalled. The story, now in its third installment, exposes the harsh realities associated with internet chat rooms and websites - specifically how sexual predators are using these sites to stalk unsuspecting teenagers.

Special agents posing as 13 to 15 year old children set up an internet sting operation. The operation, conducted from a typical suburban neighborhood home, was the meeting place where these online predators could meet their prey. With cameras rolling, hundreds of men of all ages and all walks of life converged on the house. The predator was welcomed into the home where they thought they were going to meet the teenager for a sexual liaison. Instead, they were greeted by an NBC reporter. The reporter confronted the men and asked why they were there. They tried to lie of course, however, the reporter was armed with the chat logs from the conversations they'd been having with the special agents. At the conclusion of the reporters questioning, the men were allowed to leave the home only to meet up with law enforcement outside where they were arrested.

As I watched in complete disgust, I couldn't help but think of all the parents out there that do not know what their children are chatting about or who they may be chatting with online. I'm sure the majority feel it can't happen to their daughter or son—they're good kids and smarter than that. Innocent, and even the not so innocent, teenagers are no match for these cold, calculating, and certainly cunning career criminals.

So what can you do as parents? First, be aware of the signs that your child may be at risk.

- Does your child spend large amounts of time on-line, especially at night?
- Have you found pornography on your child's computer?
- Does your child receive phone calls from anyone you don't know or is making calls to numbers you don't recognize?
- Does your child receive mail, gifts, or packages from someone you don't know?
- Has your child become withdrawn from the family?

Get involved and stay involved. Check out the Department of Justice/FBI webpage (http://www.fbi.gov/publications/pguide/pguidee.htm) to get more information about what you can do as parents. Protect your children by knowing what to do if you suspect they are being targeted by Online Predators. They don't have to become victims.

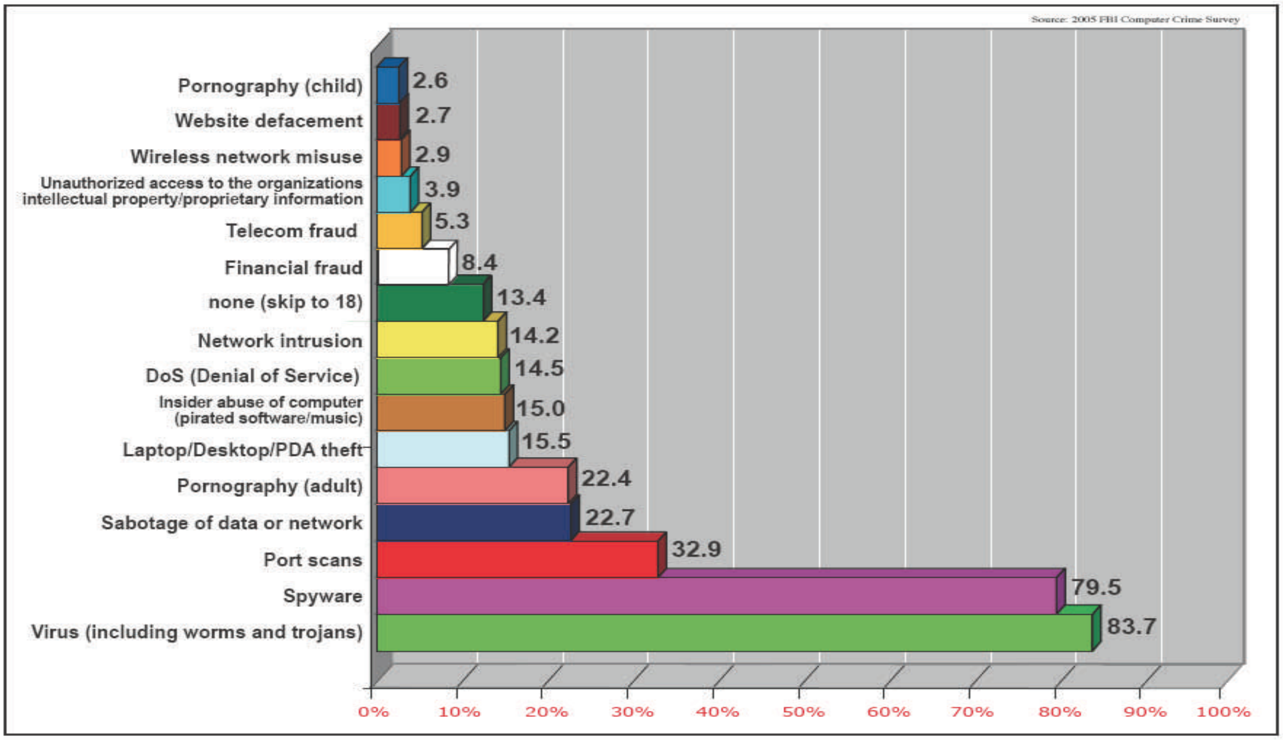
AND THE SURVEY SAYS!

Each year the FBI conducts a computer crime survey whereby it asks various organizations to respond to a number of questions concerning the types of security incidents they are experiencing. A total of 2,066 organizations were involved in the 2005 Survey. What follows is an analysis of the various incidents organizations are finding on their networks.

Which types of computer security incidents has your organization detected within the last 12 months?

An analysis of the responses to this question indicate that the vast majority of respondents (87%) experienced some type of computer security incident. The average responding organization experienced several (2.75) different types of computer security incidents with each type potentially occurring multiple times (such as viruses and port scans) to an organization. Over 79% had been affected by spyware and not surprisingly almost 84% had been affected by a virus attack at least one time within the last 12 months, despite the 98% almost universal usage of Antivirus software. Port scans being at only 33% is a strong indicator that many respondents are not detecting the almost unavoidable port scans most networks experience. This may imply that even the 5,389 reported computer security incident types indicated by individual organizations may be significantly lower than the actual number. As expected, adult pornography was fairly high on the list of incident types at number five (395 responses) out of fifteen, with over 22% of organizations dealing with this issue. Although adult pornography is not illegal as child pornography is, it is against the policy of most organizations.

New York had the lowest percentage of organizations experiencing unauthorized access, but the highest percentage of experiencing insider abuse, laptop theft, telecom fraud, viruses, and website defacement. Austin, being the most high tech area surveyed, was home to the organizations most likely (over 91%) to have at least one type of computer security incident. **2039** respondents (**1762** respondents not including the 'None' responses)



Source: 2005 FBI Computer Crime Survey

THE TREASURES OF TROY

A Security Perspective by: Robin Proctor

Between 1300 and 1200 BC, according to Greek mythology, the Greeks waged war against the City of Troy. Troy was known to be rich in treasure. The Trojans built massive walls around the city in its defense. The Greeks defeated the Trojans in many battles, but could never break through the walls of Troy.

Seeking to gain entrance to Troy, Odysseus, a cunning and clever man, ordered a large wooden horse to be built. The inside was hollow where soldiers could hide. Once the statue had been built, Odysseus and a number of Greek warriors climbed inside. The Greek fleet sailed away hoping to deceive the Trojans. They left behind one man, a Greek spy named Sinon. Sinon was to trick the Trojans into believing the wooden horse was safe and would bring them good luck. Celebrating their perceived victory, the Trojans dragged their trophy into the city behind the very walls that had kept them safe.

When the time was right, probably while the city was sleeping; Sinon opened a secret door and freed Odysseus and the Greek warriors from the wooden horse. They slaughtered the Trojans, ravaged the City of Troy, and stole their treasures.

Welcome to the 21st century. The clever ruse designed by Odysseus is no longer just a myth; it is a serious threat to Network Security. According to industry security experts, the biggest security vulnerability facing computer users and networks is email with concealed Trojan Horse software—destructive programs that masquerade as benign applications and embedded links to seemingly innocent websites that download malicious code. In 2005, targeted Trojan attacks - as opposed to computer worm outbreaks - became a greater concern. Unlike the more indiscriminate assaults by viruses and worms, Trojans can be delivered with precision to target organizations network infrastructure.

Security experts believe the most important line of defense in computer security is the user. User training and awareness about social engineering attack techniques and safe web browsing practices are integral to a sound computer security posture. Social Engineering makes attacks easier. Recent Trojan Horse attacks have been similar in using social engineering methods to enter the targeted computer network. Social engineering exploits the weakest link in computer network defense—the user—by persuading or deceiving the user, through trust or intimidation, to act out of character.

So what can you (the user) do to help prevent these sorts of attacks and defend our Network? ALL users should be wary of emails with ANY of the following characteristics:

◊ Email messages written as if they are part of an ongoing conversation, but the user was never part of the original thread.

◊ Email messages disseminated by people or organizations with whom the user never has had contact or that entice the user to click on a link or open an attachment for more information.

◊ Emails with attachments the user was not expecting. This can be any type of attachment, including files with common extensions, such as “.doc” for Microsoft Word files, “.jpg” for photo files, and “.wmv” for video files.

◊ Emails that claim to originate from someone familiar to the user, but the “From” displays differently than in previous messages, such as with a misspelled name or only an email address instead of the sender’ name.

◊ Email messages that do not display the recipient in either the “To:” or “cc:” fields, or have unfamiliar people in the “To:” field.

TROY - (CONTD)

While firewall architecture (the walls of Troy) blocks direct attacks, email (with an embedded Trojan Horse) provides a vulnerable route into an organization's internal network (the city of Troy) through which attackers can destroy or steal information (our treasure).

Look before you click. In today's world of Cyber Crime, theft of proprietary information is BIG business. Don't let the Odysseus of today lure you into a false sense of security. If you receive any suspicious email, please DO NOT open it. Send it to COTSecurityServicesISS@ky.gov by opening a new email message, then drag and drop the suspicious email as an attachment.

SECURITY INCIDENTS?

A security incident can be defined as any adverse event threatening computer security. The adverse event may potentially lead to loss of data confidentiality, compromised data or system integrity, or decreased availability and/or denial of access to an information system and/or network. Incidents generally fall into two categories: physical and electronic.

Physical security incidents include, but are not limited to, breaches of physical security policies such as unauthorized access to a facility; theft or damage to computer equipment or media; bomb threats; or natural disasters such as a fire, flood, or tornado.

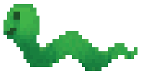
Electronic security incidents include any suspicious activity (malicious or benign) that may jeopardize the security of the KIH networks, servers, workstations, or other computing resources or that violates enterprise policies. Examples include, but are not limited to, unauthorized computer access; inappropriate computer use (surfing pornographic websites, using Commonwealth computer resources for non-business related activity, etc.); cyber attacks; website defacements; sending or forwarding spam, pornographic email, or chain letters; or exposure to computer viruses or other malicious code.

If you encounter an incident that you feel is suspicious, report it immediately to COTSecurityServicesISS@ky.gov. Only through diligence and cooperation can the Commonwealth protect and preserve the integrity of its computing environment.

IS IT A VIRUS OR A WORM?

Viruses are small programs written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

- It must execute itself. It will often place its own code in the path of execution of another program.
- It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file.
- Viruses can infect desktop computers and network servers alike.



Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm.

WHAT IS SPYWARE?

Some people mistake spyware for a computer virus. A computer virus is a piece of code designed to replicate itself as many times as possible, spreading from one host computer to any other computers connected to it. It usually has a payload that may damage your personal files or even your operating system.

Spyware, on the other hand, is generally not designed to damage your computer. Spyware is broadly defined as any program that gets into your computer without permission and hides in the background while it makes unwanted changes to your user experience. The damage it does is more a by-product of its main mission, which is to serve you targeted advertisements or make your browser display certain sites or search results.

At present, most spyware targets only the Windows operating system. Some of the more notorious spyware companies include Gator, Bonzi Buddy, 180 Solutions, DirectRevenue, Cydoor, CoolWebSearch, Xupiter, XXXDial and Euniverse.

How Did it Get on Your Computer?

Spyware usually gets onto your machine because of something you do, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. These applications often use trickery to get you to install them, from fake system alert messages to buttons that say "cancel" when they really do the opposite.

Here are some of the general ways in which Spyware finds its way into your computer:

Piggybacked software installation - Some applications -- particularly peer-to-peer file-sharing clients -- will install spyware as a part of their standard install. If you don't read the installation list closely, you might not notice that you're getting more than the file-sharing application you want. This is especially true of the "free" versions that are advertised as an alternative to software you have to buy. There's no such thing as a free lunch.

Source: How Spyware Works, HowStuffWorks (http://www.howstuffworks.com), by Dave Coustan. HowStuffWorks, Inc., 2005.

DID YOU KNOW?

Top 10 spam producing countries, according to Sophos

1. United States
2. South Korea
3. China (including Hong Kong)
4. France
5. Spain
6. Canada
7. Japan
8. Brazil
9. United Kingdom
10. Germany

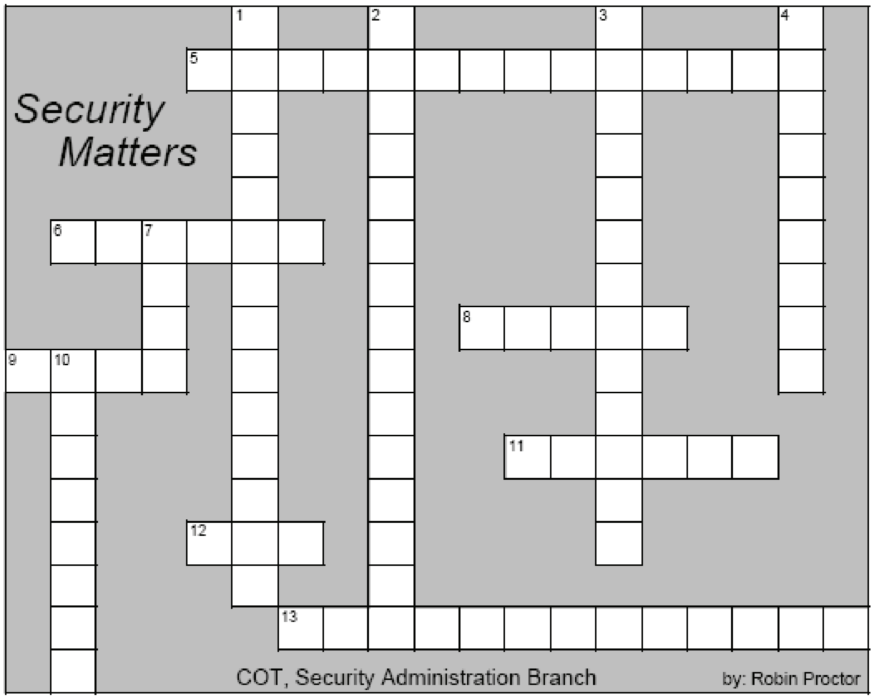
Other "Ware"

- **Malware** - a general term for any program that makes changes (does malicious or "bad" things) without your express permission
- **Adware** - programs designed specifically to deliver unrequested advertising
- **Stealware** - specific spyware designed to capture clicks or Web-site referral credits
- **Browser hijacker** - a malicious program that becomes deeply embedded in your browser's code and core functionality

Did You Know . . .

According to ClickZ Stats, 80 percent of spam is likely generated from zombie PCs that are controlled by spam Trojan horses. These destructive programs are usually installed by worms or spyware without the user's knowledge.

TEST YOUR SECURITY KNOWLEDGE



Across

5 - A means of user verification.

6 - It can monitor and profile your web usage and direct pop up ads based on your surfing habits.

8 - A self-replication program that spreads by inserting copies of itself into other executable code or documents.

9 - Unsolicited e-mail.

11 - A program, usually installed on a computer without the owners knowledge, that allows another person elsewhere on the internet to make use of your computer.

12 - An automated program that accesses a web site and traverses through the site by following links present on the pages.

13 - Stealing victims' personal information and credentials.

Down

1 - An anomalous condition where a program somehow writes data beyond the allocated end of a buffer in memory.

2 - A type of attack that attempts to block a network service by overloading the server.

3 - Hardware, software, or firmware that is intentionally included in a system for an unauthorized purpose.

4 - Software consisting of computer programs that attempt to identify, thwart, and eliminate computer viruses and other malicious software (malware).

7 - A self-contained and self-replicating program that does not need to be a part of another program to propagate itself.

10 - A code which authorizes access to protected networks, systems or files.

1 - Buffer Overflow, 2 - Denial Of Service,
3 - Malicious Code, 4 - Anti Virus
5 - Authentication, 6 - Adware, 7 - Worm,
8 - Virus, 9 - Spam, 10 - Password,
11 - Trojan, 12 - Bot, 13 - Identity Theft

CYBER BYTES

Trojan blitz poses as credit card warning

UK businesses faced a barrage of 115,000 emails containing a new Trojan on Friday, 22 January before anti-virus vendors scrambled out an update, according to email filtering firm BlackSpider Technologies.

The Trojan downloader malware - called Agent-ADO - comes in the payload to a message that poses as a warning about a user's credit card limits been exceeded.

Infected emails commonly have the subject line "ERROR:YOUR CREDIT CARD OVERDRAFT EXCEED!" and an infected attachment, a packed executable file called FILE1185 which is 5592 bytes long. Analysis of the malware is ongoing. Sysadmins are encouraged to set up rules to block the malware at the gateway. The rest of you: resist the temptation to open the attachments of unsolicited emails. Read complete article at: http://www.theregister.co.uk/2006/01/23/trojan_blitz/

Copyright: The Register 2005 (www.theregister.com)

Google vs. government

In a move to bolster its case against pornography, the Bush administration requested an order from a federal judge yesterday which would force Google to reveal information about surfing habits.

The court papers detail Google's refusal to reveal data, including all searches made on Google in any one-week period, and 1 million random URLs. Counsel for Google has vowed to fight the government in order to preserve trade secrets and the privacy of its users, according to The Mercury News. Read complete article at: http://www.securityfocus.com/brief/111

Copyright: Security Focus 2005 (http://www.securityfocus.com)

What guidelines can you follow when publishing information on the internet?

Realize that you can't take it back - Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages so that they open faster; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you can't guarantee that you can completely remove it. Read complete Cyber Security Tip STO5-013

Produced 2005 by US-CERT , a government organization (www.us-cert .gov)

Understanding Bluetooth Technology

Bluetooth is a technology that allows devices to communicate with each other without cables or wires. It is an electronics "standard," which means that manufacturers that want to include this feature have to incorporate specific requirements into their electronic devices. These specifications ensure that the devices can recognize and interact with other devices that use the Bluetooth technology. If someone can "discover" your Bluetooth device, he or she may be able to send you unsolicited messages or abuse your Bluetooth service, which could cause you to be charged extra fees. Worse, an attacker may be able to find a way to access or corrupt your data. To find out more about how you can protect yourself, read complete Cyber Security Tip STO5-015

Produced 2005 by US-CERT , a government organization (www.us-cert .gov)

We’re on the Web: http://cot.ky.gov/

About COT:

Mission

“To provide leadership in the use of information technology to enhance government services, improve decision making, promote efficiency and eliminate waste.”

Values

- Adopt an Enterprise Approach to planning, investing in, and managing information technology for the commonwealth.
- Provide information technology as a “utility” to state government agencies.
- Apply Principles of Enterprise Architecture and Project Management to building critical information technology systems that scale to meet commonwealth requirements.
- Promote Technology in Kentucky's educational systems.
- Support Gov. Fletcher's initiatives to attract and retain technology companies in Kentucky.

Helpful Links:

COT Security Website: http://cot.ky.gov/security/

COT Security Alerts: http://cot.ky.gov/security/security-alerts/

COT Security Forms: http://cot.ky.gov/security/security-forms/

Archived Security Awareness Newsletters: http://www.gotsource.net/dscgi/ds.py/View/Collection-4425

KY Homeland Security: http://www.homelandsecurity.ky.gov/

FAQ COT Security: http://cot.ky.gov/security/security-cot-questions/

Anti-Virus Information: http://cot.ky.gov/guide/anti-virus.htm

COT Enterprise Polices & Standards: http://cot.ky.gov/enterpriseit.htm

Useful Security URLs: http://cot.ky.gov/security/useful-security-urls/

TECHLINES Technology News: http://techlines.ky.gov/

McAfee Virus Information: http://us.mcafee.com/virusInfo/default.asp

Kentucky
UNBRIDLED SPIRIT™

Top 10 Security Tips!

The National Cyber Security Alliance created these tips as a guide to improve both home and office computer security.

http://www.staysafeonline.info/

1. Use anti-virus software and keep it up-to-date.
2. Don’t open e-mails or attachments from unknown or unexpected sources.
3. Protect your computer from Internet intruders—use “firewalls”.
4. Regularly download security updates and patches for operating systems and other software.
5. Use hard-to-guess passwords.
6. Back-up your computer data on disks or CDs regularly.
7. Don’t share access to your computers with strangers.
8. Disconnect from the Internet when not in use.
9. Check your security regularly- don’t be vulnerable to hackers and viruses.
10. Make sure your family and employees know what to do if your computer becomes infected.

Commonwealth Office of Technology

101 Cold Harbor Drive
Frankfort, KY 40601
Phone: 502-564-7680
Fax: 502-564-6856
Contact COT at: http://cot.ky.gov/