

Insight to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter



Zero Day Attacks

IBM warns 'zero-day' hacker exploits growing. Hackers are exploiting users' inability to comply promptly against announced vulnerabilities, according to an IBM security report. According to IBM's X-Force midyear report, more than 90 percent of browser-related exploits detected during the first six months of this year have occurred within 24 hours after these vulnerabilities were disclosed. More significantly, IBM noted hackers are adopting new techniques and strategies in order to better exploit "zero-day" vulnerabilities, or simply before users are even aware they need to install patches or updates. Also, "exploit codes" being made public further compromise IT systems. In the first six months of 2008, nearly 80 percent of Web browser exploits are targeted browser plug-ins. From Infragard & hackerinthebox

UPDATE your computers!
UPDATE your applications!
 Most updates are security related.

In this Issue:

Recent Malicious Activity	1,2
Virus on Space Station	1
Firewall Basics	3,4
New "Sick" E-mail Scam	4
Security Links	4

Recent Malicious Activity (from MS-ISAC)

Users of the internet have experienced an increasing amount of malicious threats; to include increases in Phishing, SQL Injection, DNS Cache Poisoning and Attempts To Exploit Current Events.

I. Phishing

Beginning on August 5, 2008 reports of mass emails claiming to be from the CNN.com news Web site began to surface. Currently the subject of the email is "CNN.com Daily Top 10". These emails are not from CNN, and contain web links to malicious sites that will attempt to install malware purporting to be an Adobe Flash Player upgrade. The



MS-ISAC has received reports from multiple states including Michigan, New York, North Carolina and Wisconsin, indicating their users have received these emails.

These emails have been circumventing spam filters and utilizing html based messages including the CNN web site logo and very enticing headlines to lure unsuspecting recipients into clicking on the links for news stories which are actu-

ally downloads of malware from various web sites. Reports indicate that hundreds of web servers may be compromised and hosting this malicious content. The use of news and current events are a proven and effective social engineering tool.

When the 2008 Olympics started Friday, August 8, we anticipate spammers, phishers, and other online attackers



used bogus "Olympic-themed" headlines in their scams. Organizations must realize that Phishers use this technique during holidays or special events regularly

II. SQL Injection Attacks

Some states (including Idaho) have reported a high volume of SQL injection attacks targeting ColdFusion (.cfm) web applications, originating from a number of IP addresses. Based on an analysis of the attacks, compromised web sites may contain injected HTML content that re-directs users to web sites with malicious content. (Continued on page 2)

Virus Found in laptop in Space Station (from Infragard and DB Techno)

You can't even go into space to get away from computer security threats these days!!

It was confirmed on Wednesday by NASA that they discovered a computer virus on a laptop that is aboard the International Space Station. The virus was first discovered by Symantec on August 27. Symantec refers to this worm as



W32.Gammima.AG. It impacts systems running Windows 2000, 95, 98, Me, NT, XP, and Windows Server 2003. NASA isn't concerned that the virus poses a direct threat to them, since the laptop was a stand-alone system and is not used for official work.

W32.Gammima.AG is a worm that can be spread through removable media, such as thumb drives and it has the ability to steal passwords, particularly on-line gaming passwords.



Warning:
Do NOT believe in e-mailed warnings about viruses or other security risks that ask you to forward them on to all your friends or coworkers. Check with your IT personnel or go to www.snopes.com

Security shouldn't slow you



down, it should make you more confident as you move forward.

Recent Malicious Activity (from page 1)

News reports indicate thousands of web sites have been recently compromised by SQL injection attacks.

III. DNS Cache-Poisoning

One state has reported the possible DNS-cache poisoning of a (non-state government) third-party partner. This is being investigated further. However, we recommend that all states review the details of the recently disclosed DNS cache poisoning vulnerabilities and ensure that their critical DNS servers have been patched. (*Idaho agencies have responded well to this threat*)

IV. Other Current Cyber Events

The CNET Clientside Developer Blog has been compromised and was hosting malicious JavaScript that attempted to exploit vulnerability in multiple versions of Adobe Flash.

Recommendations:

We recommend that all of the following actions be considered:

- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Exercise caution when previewing or opening suspicious and unsolicited email messages.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Update your anti-virus software signatures on all desktops, laptops and servers as soon and as frequently as possible.
- If possible, change global default email options so that all mail is viewed in text format. This provides an opportunity for end users to see the email without all the trusted brand logos and potentially avoid becoming a phishing victim. (*Idaho agencies should consider this if it meets their business needs*)
- Immediately review your DNS infrastructure and apply the necessary patches and workarounds after appropriate testing. (*Idaho has addressed this*)

References:

Adobe

http://blogs.adobe.com/psirt/2008/08/verifying_installers.html

US-CERT

<http://www.us-cert.gov/>

MX Logic

<http://www.mxlogic.com/itsecurityblog/1/2008/08/Spam-Alert-Huge-Volumes-of-Fake-CNN-News-Updates.cfm>

SANS

<http://isc.sans.org/diary.html?storyid=4771>

The Register

http://www.theregister.co.uk/2008/08/07/new_sql_attacks/

Firewalls—Why you need one (from MS-ISAC)

What is a firewall and why should I use one?

A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. Firewalls add a layer of protection by blocking unauthorized and potentially dangerous data from entering your computer or network. Firewalls are especially critical for users who have an “always on” connection to the Internet.

Some users may think that data residing on their computer is not valuable and therefore a firewall is not necessary. However, even small pieces of information can be obtained by the hacker and used



to steal identities and other personal data. In addition, hackers may be interested in taking over your computer to store illegal materials or launch other attacks that can leave a trail back to your computer. Once a hacker gets access to your computer, the intruder may have access to resources and data stored on your machine.

What does a firewall protect me from?

Firewalls can help protect your data and computer by blocking the following:

- unsolicited traffic/malware from coming into your computer or network
- traffic from known malicious computers
- specific traffic you don't want leaving your computer or network
- programs, protocols and ports that you specify
- attempts to access or attack your computer

Firewalls can also log activity, and these logs should be reviewed periodically to identify any anomalous or unexpected activity.

What type of firewall should I use?

There are two types of firewalls: hardware and software. A hardware firewall is usually an external device that sits between your computer and your connection to the Internet. A software firewall (also known as a personal firewall) runs directly on your computer. This firewall is the most common type for home users.

The selection of a firewall is dependent on what is being protected. The value of the assets, the complexity of the computers or networks, and their usage of the Internet will dictate the type and size of firewall that should be used.

Make sure you have a firewall--selected based on your business or personal needs--and that it is enabled.

Before enabling a firewall, read the documentation carefully to ensure proper configuration. A properly configured firewall can save you hours of recovery or rebuilding of data.

Below are some areas for consideration when installing a firewall:

- allow only the traffic that you need
- enable the “automatic update” feature if one exists and also periodically check the firewall vendor's website for the latest software updates
- enable the logging feature and review the logs regularly
- change default administrator accounts (if available) and password
- disable the remote management option (if available)

A firewall is a very valuable tool to protect your data and your computers, but it must be selected, installed, configured, monitored, and maintained effectively to do its job. It's also important to note that although firewalls can block intruders, viruses or unwanted (Continued on Page 4)



Hacker Safe promises, often lead you into a false sense of security, making you an even better target for the hackers. Hackers love to break into “Hacker Safe” sites.

**CHECK OUT
THESE
LINKS**

Links to top Security Websites:

Good websites to surf:

<http://www.sans.org/>

<http://www.cert.org/>

<http://www.msisac.org/>

<http://csrc.nist.gov/>

<http://www.issa.org/>

<http://www.infragard.net/>

<http://www.ic3.gov/>

<http://www.securityfocus.com/>

<http://www.snopes.com/>

<http://>

www.nationalterroralert.com/

**Internet Security is
not an obstacle, it's
the path to freedom
and flexibility.**

New, Abhorrent E-mail Scam: “We Kidnapped Your Child”

From Infragard and PC World

The Bad Guys really know how to push our buttons.

PC Advisor reports that Hackers have begun to resort to really low-level psychological schemes to gain our attention and steal our money through snatching private information from our computers. There is a new ‘sick’ kidnap spam e-mail that many parents will not be able to ignore.

Hackers are sending e-mails claiming they have kidnapped the receiver’s child. This is all an attempt to infect PCs with a Trojan Horse virus, said security firm Sophos. The security firm is warning users that emails entitled ‘We have hijacked your baby’ are being sent to Web users around the globe. As well as asking for a US\$50,000 ransom for the ‘release’ of the child, the messages also contain an attachment supposed to be a photograph of the child. Instead the file actually contains a deadly Trojan Horse that will steal personal information.

Never trust e-mails sent by people you do not know, particularly if they have links or attachments. Never click on those links and never open the attachments.

Firewalls (cont. from page 3)

traffic from getting into your computer, using a firewall is not a complete solution to security. Firewalls should be used along with anti-virus, anti-spyware, and anti-spam software, as part of a defense-in-depth strategy for protecting your computer from various forms of malware (viruses, worms, trojans, etc.), hackers, and others who want your data or your computer for illegal or malicious purposes.

Remember: Cyber Security is Your Responsibility. Always apply safe cyber security practices to protect the data on your computer or network.



References

To learn more about firewalls, please visit the following sites:

MS-ISAC - Beginners Guide to Firewalls

<http://www.cscic.state.ny.us/localgov/#download>

US-CERT

<http://www.us-cert.gov/cas/tips/ST04-004.html>

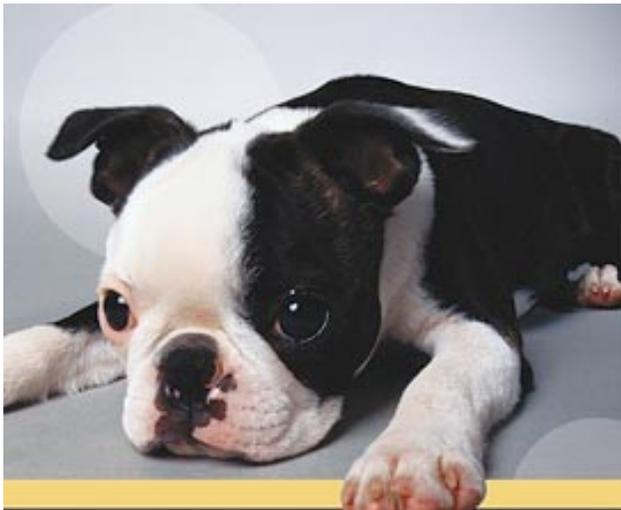
How Stuff Works - Firewalls

<http://computer.howstuffworks.com/firewall.htm>

Firewalls for Dummies

<http://www.dummies.com/WileyCDA/DummiesTitle/Firewalls-For-Dummies-2nd-Edition.productCd-0764540483.html>

Some Great Security Posters from other organizations.



Someone discovered my **PASSWORD.**
Now I have to rename my dog.

Use strong passwords. A simple password, such as your pet's name, is not sufficient protection. Hackers systematically check every possible word to decipher passwords in no time.

Watch for an online awareness program
PUBLIC JOBS: PRIV

MINNESOTA STATE COLLEGE & UNIVERSITY SYSTEM




PASSWORDS ARE LIKE SOCKS



CHANGE THEM OFTEN

GET LAZY WITH YOUR PASSWORDS AND YOU COULD CAUSE A REAL STINK! CHANGE



www.ballarat.edu.au/is

sec·U·R·I·T·y



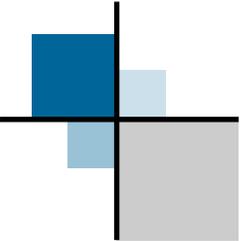
Laptop: \$1800
Cell phone: \$79
Backpack: \$69
Books, supplies: \$150

Identity Theft: Priceless

YOU ARE IT!



THE UNIVERSITY OF ARIZONA,
INFORMATION SECURITY OFFICE
security.arizona.edu



Contact us at 322-1505 or servicedesk@cio.idaho.gov

