SECUREPURDUE NEWS
www.purdue.edu/securepurdue

January 2008
Volume 1, Issue 14

All the news that's secure to print.

Patch Tuesday

by Bill Harshbarger

On the second Tuesday of every month, Microsoft releases security related patches for its products in response to vulnerabilities that could be leveraged by attackers. The release schedule of patches and notification is commonly known as "Patch Tuesday. " Typically, a large percentage of the patches released address some security or reliability issue that exists in Microsoft operating systems or other software like Office or SQL Server. Acting on Patch Tuesday is important because there are real consequences for not promptly applying patches when released. Often times, an exploit for the vulnerability being patched is created within weeks or days of release of the patch. In fact, over the past few years, this time between patch and exploit has been decreasing towards a few hours. Due to the relative swiftness from patch to exploit, the day after Patch Tuesday is referred to as "Exploit Wednesday."

Exploit Wednesday represents the start of the attacker's opportunity to begin reverse engineering the patches and exploiting the newly published vulnerabilities. Since the time it takes attackers to accomplish this is also rapidly decreasing, it is extremely important to ensure all security patches released by Microsoft be installed as soon as possible. While not specifically a result of 'Exploit Wednesday', systems may also be exposed to newly discovered vulnerabilities for a time before the next round of patches, or to ones that have not yet been addressed by a patch. It is essential to have other measures such as firewalls, antivirus, and user account restrictions in place to mitigate this risk.

See Patch Tuesday on page 4

In this issue

FROM the CISO

By Scott Ksander
Executive Director
IT Networks & Security

Every now and then the cosmos gives us a sign that lifts our spirits. Many of you helped give me that sign over the past month and I want to thank you for that. Recently we had a number of very targeted attempts to attract Purdue people to undesirable web sites for the purpose of gathering identity information. Most of these were requests to "just click here" with the promise that something "wonderful" would come your way. The great news was that many of you did not click and instead decided to report the problem to abuse@purdue.edu.

I don't believe this would have been the case 12-18 months ago and it is a great sign that our security outreach efforts on campus are working. Thank you!! Please keep up the good work and tell all your coworkers, friends, and

See CISO, Page 2

Have you been "Rickroll'd" lately?

CISO from Page 1

A "friend" sends you an Instant Message or an email with a link that is supposed to take you to something of interest. Instead, if you click on this link it takes the viewer to a video of "Never Gonna' Give You Up" sung by 80's pop star Rick Astley. Once you click on the link and are taken to the Rick Astley video website, you have been officially "Rick Rolled." This is usually done with YouTube videos related to unconfirmed gaming news. However, the problem is the same for anyone who receives an unsolicited email with a link to visit something great and then they get more than they bargained for in the form of viruses or identity theft.

If you click on this link, it takes the viewer to a video of "Never gonna give you up" by Rick Astley
http://www.youtube.com/watch?v=eBGIQ7ZuuiU

• **Google Security Test**
To test Google's ability to block harmful advertising, Googles' IT security firm posted an ad that read "Is your PC virus-free? Get it infected here!" Google displayed the advertisment 259,723 times; 409 web surfers actually clicked on the ad.

It is a new year but don't forget our campaign, ***Don't Just Click It.*** We need to caution the University community from clicking on URL links in emails or Instant Messages (IM) or e-greeting messages sent to you. Clicking on links in an email or IM can take you to a fraudulent website in an attempt to steal your personal information.

A suspicious message may start with a key phrase: "Click the link below to gain access to your account." The links that you are urged to click may contain all or part of a real company's name and are usually "masked," meaning that the link you see does not take you to that address but somewhere different, usually a phony site. To view the real web address, rest your mouse pointer on the company's Web address.

Install up-to-date antivirus and antispyware software.
Some phishing e-mail contain malicious or unwanted software that can track your activities or simply slow your computer.

Purdue provides free anti-virus software for students, staff, and faculty. This is intended for use on non-Purdue owned equipment (Windows machines), which students, faculty and staff can download. Purdue offers two versions of VirusScan, one for Purdue computers and one for non-Purdue computers.

Unfortunately, not all malicious or unwanted software can be prevented with antivirus or antispyware software. So, take precautions to not infect your computer or your network.

family. Maybe you can use the example of being "Rickroll'd" that appears in this issue to illustrate the point.

During a presentation at one of our October Security Awareness Month events I discussed the "black market" for identity and authentication information from an economic point of view. This clearly indicated that, while we may be making progress, we have a long way to go.

Current estimates are that the black market profits from identity trading in 2007 will be about $100 million. This is simply the money involved in the resale of identity and authentication information. It does NOT include any of the value that might have been acquired when fraudulent identities were actually used. This level of profits is equivalent to a legitimate corporate entity capitalized at about $7 billion dollars! In this "business" the number of markets around the world is increasing. The market liquidity is increasing both in terms of information and the number of criminals participating. The price of the product is decreasing (average identity purchase is down to $14 in 2007 from $150 in 2002) and the quality

CISO continues on Page 3

SPOTLIGHT

SecurePurdue Token

The Identity and Access Management Office has launched a two-factor authentication pilot using the RSA SecurID® product. The pilot project is an exploration of ways to improve security for accessing the OnePurdue portal.

Most Purdue IT systems require you to enter your career account login name and password to log in. Anyone who guesses or steals your password can then log in to the same systems as you.

By contrast, an RSA token generates a number that changes every minute. This number, combined with a PIN (personal identification number), becomes a "one-time" password to access the OnePurdue portal. This is more secure because an attacker would have to guess a PIN and steal a token to log in. Currently, the token works with the SAP portal only and allows the user to bypass changing their password every 30 days. The SecurePurdue token allows the user to enter a pin number and the token-generated number in place of their career account password.

Additional information about the SecurePurdue token, as well as future rollout plans will be announced on the SecurePurdue web site. Click on Purdue Career Account link and then SecurePurdue Token link.

CISO column from Page 2

of the product is increasing with more accurate, fully qualified identities now available. Any economist will tell you that these factors all indicate an efficient market with solid potential. In short, the bad guys are improving too.

January is a time for New Year's resolutions. Within the last week, I read suggested resolutions to improve health, ues less energy and how to keep a pet safe. It seems only appropriate that I offer a few suggested resolutions that you can make to help improve the quality of your cyber security life.

• Always read, understand and follow all safety instructions with new cyber software and tools (apologies to Norm from "The New Yankee Workshop")

• If you wouldn't post the same information or picture on the front door of your house, don't post it in electronic forum or social networking site.

• Never "just click here" unless you are 100% sure where the adventure will take you.

As always, thank you for reading, and be careful out there.

STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at:

http://www.purdue.edu/securepurdue/steam/

Top 10 Purdue email viruses

(30-day snapshot as of December 20)

Viruses	Occurrences in past 30 days
W32/MyDoom-O	289
Mal/Iframe-F	103
W32/Netsky-P	46
W32/Mytob-E	192
W32/Mytob-CN	63
Mal/ObfJS-C	516

MILESTONES

SANS 519 Web Applications Security Training

On December 18 and 19, twenty one IT staff attended a two day training on SANS Web Applications Security here at Purdue. Purdue hosted the instructor, Johannes Ullrich, for the Interactive Video Conference (IVC)training event that connected Purdue to 14 other sites throughout the nation, from the East coast to the West coast.

In July, Purdue participated in a pilot of the SANS IVC method of presenting training for VISTA training. Those participating in the training felt it was an effective means of attending training that was both cost effective and provided just in time training options. SANS has worked with educational institutions to provide less expensive training options for their staff. Without the EDU discount, the SANS 519 training would have cost $2145 per person and our staff paid only $500 for the training saving the University $32,9000 and providing much needed computer security training.

For the SANS 519 training, those in attendance could opt to register to take the certification test to earn the GWAS certificate. Fifteen of the twenty one Purdue staff opted to test for the certification.

This is the third SANS training offered in 2007 for the IT community at Purdue. We are striving to provide training opportunities that are relevant and cost effective for our staff. Some departments have small staffs and only a few can be away at a time to attend training. This allows the staff to still be near their work site yet attend training to update their skills and offer the University community more effective protection and security.

SECURITY RESOURCES

Use the following resources to educate yourself about security and privacy issues surrounding computers and data networks.

- **Secure Purdue**
http://www.purdue.edu/securepurdue then click on the Downloads link
- **Windows Update**
http://www.update.microsoft.com
- **Microsoft Baseline Security Analyzer**
http://www.microsoft.com/technet/security/tools/mbsahome.mspx
- **Windows Server Update Services**
http://technet.microsoft.com/en-us/wsus/default.aspx

Patch Tuesday from Page 1

At Purdue, Patch Tuesday affects everyone who uses Microsoft software on the campus network. Centralized patching software is in place for most managed Windows systems, but this does not ensure that every potential Microsoft system using the network is fully patched. It is important that anyone using Microsoft software be aware of these monthly patches, and make regular patching part of their security checklist. There are many free tools that users of Microsoft products can implement to ensure that patches are applied on a regular basis, including Windows Update, Microsoft Baseline Security Analyzer, Windows Server Update Services, and Automatic Updates.

While patching helps to improve security, there is a trade off. Due to the nature of the Windows operating system, most patch installs will require a reboot. This does cause an outage for a short time, but this can be compensated for by performing patches during non-peak usage hours, or relying on backup systems to keep services up while systems are patched. Patching is an important part of the overall process of securing computers, and by installing these patches quickly we help to ensure that vulnerable software does not become an avenue for attackers.