In This Issue


1. From the Trenches

John Y. at a US community college writes us:

A computer used by one of our staff was compromised in December, and began sending email advertisements for Viagra and Cialis to large numbers of addresses. We caught it fairly quickly because we have monitors that look for that kind of behavior on our network. An analysis of the computer showed that it had been infected when the user visited a small Mom-and-Pop type arts & crafts store on the web. The Mom-and-Pop website had been “re-programmed” by someone in Ukraine to send a blast of software attacks at anyone unlucky enough to visit it. One of these attacks was directed against a vulnerability in a version of Apple QuickTime released just two weeks before the attack. Symantec Anti-Virus stopped all of the attacks except the QuickTime attack. Sadly, it only takes one successful attack to compromise any computer.

Lessons We Learned

Small Mom-and-Pop websites can pose a greater risk than the sites of big vendors like Amazon.com. Owners of small businesses often don’t have the expertise or resources to protect their sites from being compromised and used by Bad Guys. Once a website has been compromised, it can then be used to attack your computer.

Anti-virus is still a necessary defense, but it can’t do the whole job. In the past, computer criminals wrote viruses that broadcast themselves all over the Internet, making it easier for anti-virus companies to identify them and develop a countermeasure quickly. Now, attacks are much more targeted and the criminals have gotten better at making attack software that is harder to detect. Anti-virus makers are finding it difficult to keep up with the criminals.

Bad Guys are targeting many applications that run on your computer, as well as the operating system. The campus computer that was compromised was completely up-to-date with its Windows security patches. But in order to keep your computer secure (besides patching Windows, Internet Explorer, and Office, all done automatically through update.microsoft.com), you have to patch commonly installed applications like QuickTime, RealPlayer, Adobe Reader, Adobe Flash Player, and Sun Java, all of which can be attacked through your email or web browser.

[Editor’s note (Wyman): Many thanks to John Y. for sharing this security story from the trenches and some valuable lessons learned. I’ll suggest two more. The compromise of the original computer might have been avoided if good-quality anti-spyware had been installed, running, and up-to-date, supplementing the protection offered by the anti-virus software in place. The threat to other computers could have been minimized or eliminated if good-quality, two-way firewall software had been installed. It could have kept the compromised computer from sending out spam and infected emails, and alerted the user of the compromised computer that something was amiss.

Here are some links you can use to patch and update software likely to be installed on your computer.
2. Malware

MonaRonaDona aka Unigray. An annoying, but otherwise fairly harmless virus whose sole purpose is to prompt the user to enter the term "MonaRonaDona" into a search engine so they can find an application that can remove the unwelcome threat. The threat will stop a bevy of applications if their name appears in the Windows title bar, including Date and Time, Windows Task Manager, Windows Media Player, Microsoft Office, Microsoft Excel, Microsoft Word and Windows Live Messenger. Once you enter the name 'MonaRonaDona' into an Internet search engine, some of the top search results will be the "fix" that the malware authors have probably also conveniently created in order to solve the problem.

More information:
http://www.symantec.com/enterprise/security_response/weblog/2008/03/monaronadona_the_pure_social_e.html
http://blog.washingtonpost.com/securityfix/2008/03/the_411_on_the_monaronadona_ex.html

3. Scams and Hoaxes

PayPal Security Message Phishing Scam
Part of a new crop of relatively plain and simple scam email messages, but no less dangerous for unwary web users. The email states simply that the recipient has one security-related message waiting. The recipient is instructed to click a link, ostensibly to retrieve the security message and “resolve the problem.” In fact, the link takes you to a fake login page that asks you to provide account details and other personal information. Fake web pages like these come and go, and may no longer be online by the time you receive the email.


Email Attacks Target Pro-Tibetan Groups
Groups sympathetic to anti-Chinese protesters in Tibet are under assault by cyber attackers who are embedding malware in email that appears to come from trusted colleagues. The email is being sent to members of human-rights groups. The messages include infected attachments in PDF, Microsoft Word and PowerPoint formats that install keyloggers and other types of malware once opened. The malicious payloads have been disguised to evade detection by anti-virus scanners. Names of attached files include “UNPO Statement of Solidarity.pdf,” “Daul-Tibet intergroup meeting.doc” and “tibet_protests_map_no_icons__mar_20.ppt.”

More information: http://www.theregister.co.uk/2008/03/22/pro_tibetan_groups_targeted/

4. Security Screw-up of the Month

New England grocery chain Hannaford Brothers says a security breach has exposed 4.2 million of customers’ credit- and debit-card numbers to scammers. With 1,800 fraud cases reported so far, Hannaford said the breach began December 7, 2007 and continued until it was “contained” on March 10, 2008. Anyone who used a credit or debit card during that period at any of the chain’s 165 stores or 106 Sweetbay outlets in Florida faces potential problems, as do
customers who shopped at an undisclosed number of small grocers that stock Hannaford products. Hannaford has admitted that it first learned of the security breach a couple of weeks before it was “contained.” In a move designed to quell fears about identity theft, Hannaford has maintained that the stolen data contain “no personally identifiable information;” that is, no social security numbers, dates of birth, or home addresses of the victims, and that such information is neither collected nor stored by the merchant when a credit card is swiped.

http://www.boston.com/business/articles/2008/03/28/advanced_tactic_targeted_grocer/

[Editor’s Note (Wyman): It will be a while until we have the full story of what went wrong here. Although Hannaford insists that “no personally identifiable information” was compromised, it’s a strain on common sense how anyone could claim, with a straight face, that my credit card number and its expiration date are anything but personal information. If you wonder just what information is stored in the magstripe on your card, have a look at:

As with other big retail break-in’s, notably TJX* a year ago, the media reports about Hannaford have included the usual finger-pointing: the merchant, the chain of stores, the banks, and the credit card industry. Eyes fell quickly on the Payment Card Industry (PCI) Data Security Standards,** Hannaford and its security consultants have maintained the retailer was in compliance with PCI security standards.

Hannaford countered initially that the data were ripped off while being transmitted for approval—after they’d left the store. This would be akin to merchandise being stolen from a delivery truck while it is speeding down the highway. Later Hannaford said that the computers in their stores were infected with malicious software that hijacked credit card information as transactions were being transmitted to the banks for approval—while they were still in the store. Apparently, the stolen data were then relayed to an offshore Internet Service Provider by the same infected computers. Did the stores’ computers have good security software installed, updated, and working? Were the computers being checked routinely for unusual activity? No word on those questions yet. The big lesson here may be that while Hannaford’s computers were in compliance with the credit card industry’s specialized security standards, they were nevertheless vulnerable to plain old hacking, unequipped to defend themselves against a malware attack, or simply under-managed.

* TJX: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782
** PCI Standards: https://www.pcisecuritystandards.org/]

5. Microsoft and Apple Security Updates

Microsoft and Apple provide free security updates for their software products.

**Windows:** Microsoft issues patches for all Microsoft products on the second Tuesday of each month as well as out-of-cycle patches on any day of the month. The next scheduled release date is April 8th. Check manually too, once every two weeks, to make sure all of the updates have been installed.


**OS X:** Updates are issued frequently, and their contents may differ depending on which processor is in your Mac (PPC or Intel).


**iPhones:** Must be updated manually: http://docs.info.apple.com/article.html?artnum=305744
6. Security Newsbytes

Unpatched RealPlayer Bug Paves Way for Drive-by Downloads
An unpatched bug in RealPlayer leaves the media player open to drive-by-download attacks, which hackers can use to trick prospective victims into visiting maliciously constructed websites. The vulnerability stems from coding errors, which enable the malicious content to be played within a user's Internet Explorer browser. RealPlayer version 11.0.1 has been confirmed as vulnerable. Other versions of the media player may also be flawed. A patch is said to be forthcoming from RealNetworks, the makers of RealPlayer.

More information: [http://www.theregister.co.uk/2008/03/12/realplayer_bug/](http://www.theregister.co.uk/2008/03/12/realplayer_bug/)

Apple Releases Mega-Patch for OSX
Apple has released a security update for Mac OS X that fixes nearly 90 vulnerabilities, including a high-profile web browser and Apple Mail flaw. The set of patches addresses a variety of security flaws, including several that could let an attacker gain control over a Mac. The vulnerabilities expose Mac users to a risk that is familiar to Windows owners: the installation of malicious code through a tainted website or email because downloaded files are not properly validated. The update also modifies iChat, Apple's instant messaging application, to thwart instant message threats such as the Leap.A pest, a Mac worm first detected more than two years ago.

More information:
[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam__malware_and_vulnerabilities&articleId=9069538&taxonomyId=85](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam__malware_and_vulnerabilities&articleId=9069538&taxonomyId=85)

Mac Scareware Site Still Open for Business
The same tried-and-true social engineering tactics traditionally wielded against Windows users to frighten people into buying bogus security software are now being used to target Mac users. Security experts say the curators of macsweeper.com warn visitors that their machine is full of threats to the user's privacy, and that they need to pay $39.99 for software that removes the bogus threats. The MacSweeper site, based in Ukraine, has all the features of a scareware scam, including an Apple Support look-alike homepage and a boilerplate company message lifted straight from Symantec's corporate website. Regardless of which operating system you use, here's a good rule of thumb for applications: If you didn't go looking for it, don't install it. Never install anything that uses these types of scare tactics.

More information:
[http://blog.washingtonpost.com/securityfix/2008/01/scareware_program_targets_mac.html](http://blog.washingtonpost.com/securityfix/2008/01/scareware_program_targets_mac.html)

Pennsylvania Pulls Plug on Voter Site after Data Leak
With voting in Pennsylvania's presidential primary just a month away, the State has been forced to pull the plug on a voter registration website found to be exposing sensitive data about voters. The problem lies in an online voter registration application form designed to simplify the task of registering to vote. State residents used it to enter their information on the website, which then generated a printable form that could be mailed to State election officials. Because of a programming error, the website was allowing anyone on the Internet to view the completed forms, which contained data such as the voter's name, date of birth, driver's license number, and political party affiliation. On some forms, the last four digits of Social Security numbers could also be seen.

More information:
[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9069578&intsrc=hm_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9069578&intsrc=hm_list)