

In This Issue

1. 30th Anniversary of Spam – 2. Malware – 3. Scams and Hoaxes – 4. Microsoft and Apple Security Updates – 5. Security Newsbytes

1. 30th Anniversary of Spam

On May 3, 1978, 393 users of the US military's ARPANET (granddaddy of the Internet) received the first spam email in history. A Digital Equipment Corporation's (DEC) marketing rep, Gary Thuerk, came up with an email sales pitch that produced a fierce backlash from Arpanet administrators, as well as a small number of sales for DEC. Unsolicited bulk commercial ads moved on to Internet newsgroups, email, and website links. Much to the chagrin of Hormel Foods, the term spam was applied to the phenomenon in a pop-culture reference to a skit from Monty Python's *Flying Circus*, in which all meals in a restaurant come with spam, spam, spam and more spam. Junk email--not nourishing luncheon meat--has become the principal meaning of the word spam.

A lot has changed in the three decades since. Practically the entire online population (estimated at 1.3 billion) is subjected to a daily deluge of junk mail messages. Spam filtering technology has come a long way in the last four years in particular, but eradicating the problem has proven to be far more difficult than originally imagined. In January 2004, Bill Gates predicted that spam would be eradicated within 24 months. Microsoft's scheme called for installing better filters to weed out spam and requiring sender authentication. Microsoft wanted to see "tar-pitting" -- emails coming from unknown senders would be slowed down so that bulk mail runs would become useless.

As anti-spam defenses have advanced, so have spamming methods. Using compromised email servers, which can be blacklisted quickly, is a thing of the past as the Bad Guys have moved on to using huge networks of compromised PCs (botnets). Meanwhile, spam has begun appearing on other platforms, such as cellphones, and an estimated 95% of all email is spam. If nobody responded to spam, the tactic would not be commercially viable, but a recent survey conducted by Sophos revealed that 11% of people admit to having bought goods in response to spam. In honor of the 30th anniversary, Sophos has launched a campaign urging people to resist clicking on links in spam emails, in the hope that spam never reaches its next landmark anniversary.

More information: http://www.theregister.co.uk/2008/05/01/spam_30/
<http://www.npr.org/templates/story/story.php?storyId=90160617>
<http://www.templetons.com/brad/spam/>

Spam Tips**Don't buy ANYTHING from a spammer**

If an unexpected email brings you news that seems too good to be true, it is probably spam and a scam. If you didn't request information about the product or service, it is

probably spam and a scam. If it promises to enhance parts of your body, it won't. If it promises you a cheap and easy mortgage, you can do better by visiting your bank. If it promises that you can make a fortune on a penny stock, you can't. If you are unsure, check with five friends. Chances are four of them also received the spam and you'll know to steer clear of it.

Don't click on links in unsolicited emails

Spam filters are catching a lot of unwanted email, but some still reach you. Most spam is designed to get you to respond with your own email, click on an embedded link, or click on the link at the bottom to "unsubscribe." When you respond or click the "unsubscribe" link, the sender may add your address to a SPAM database of known active email addresses and sell it to other spammers. When you click on an embedded link, you may end up on a phony website designed to lure you into a phishing scam.

Don't be an unintentional Spammer

If you're like most people, you've probably received at least one hoax or chain letter in your inbox. What should you do with the next one you receive? Delete it! Chain letters and hoaxes have the potential to cause problems (lots of network traffic, filling up someone's inbox, or hooking you into a phishing scam), and they can also be very annoying. For current information about email hoaxes, visit <http://www.hoax-slayer.com/latest-information.html>.

2. Malware

Downloader-UA.h, a Trojan that spreads by masquerading as an MP3 music or MPEG video file available from popular file-sharing services such as Limewire and eDonkey. The malicious files are named differently in multiple languages and vary in size to make them appear like legitimate music or video files. Attempting to play one of the malicious files will trigger a program called "PLAY_MP3.exe" to download, launch, and force advertisements to appear on the infected computer.

More information: <http://blastmagazine.com/2008/05/mcafee-identifies-downloader-uah-first-medium-risk-malware-in-three-years/>

- **MalDoc-Fam**, a Trojan that is spreading through infected Word documents attached to emails posing as news about the Chinese earthquake disaster. The malware-tainted emails typically appear with body text suggesting they contain news from China's official press agency, Xinhua. Opening the attached Word document triggers an exploit that downloads malware onto vulnerable PC's.

More information: http://www.theregister.co.uk/2008/05/22/china_earthquake_trojan/

3. Scams and Hoaxes

Scammers Posing as Government Agencies Offering Protection from Scams

Phishing scams have become increasingly sophisticated in their attempts to solicit private information. Scammers are now posing as government agencies offering protection from future scamming. "The National Credit Union Administration (NCUA) and U.S. Government developed a project to protect your bank account and credit card against Internet fraud, but for this we need your help," reads one email. "You just have to register with us." A link follows that directs recipients to a fake website where they are asked to supply sensitive credit card information.

More information: <http://daily.stanford.edu/article/2008/5/22/phishingScamMoreSophisticated>

Apple Warns of Phony iPods

Apple Computer last month began notifying its service partners that some companies are illegally manufacturing digital music players that look very similar to its various Apple iPod models in an attempt to pawn them off to unsuspecting buyers. Two of the most commonly counterfeited iPods appear to be the iPod nano and the iPod shuffle. The imitation players, which often sport nonstandard headphone jacks and lack a dock connector, are sometimes stamped with the valid Apple serial number 6U545TK2TJT.

More information:

http://www.appleinsider.com/articles/06/04/19/apple_warns_of_phony_ipods.html

Phishers Target Apple iTunes Users

Phishers have been sending out spam email to iTunes users stating that they need to correct their iTunes information. Within the spam email is a link, and when the unsuspecting user clicks on it, it leads him to a website pretending to be an iTunes billing update page. The fake page asks for the iTunes user's credit card information and Social Security number, along with the mother's maiden name.

More information: <http://mac.blorge.com/2008/05/21/phishing-scam-alert-phishers-are-targeting-apple-itunes-users/>

Spammers Exploit Tragedies in China and Burma

Spammers are taking advantage of recent natural disasters to launch phishing scams and Trojans disguised as news reports and donation requests following the cyclone in Burma and the earthquake in China. Anyone attempting to donate via the suggested sites may find themselves asked for all kinds of personal and/or company information that could be used for identity theft.

More information: <http://www.vnunet.com/vnunet/news/2217415/chinese-earthquake-spawns-scams>

IRS Economic Stimulus Check Scam

The FBI has issued a warning to consumers about recently reported spam email purportedly from the Internal Revenue Service (IRS), which is actually an attempt to steal consumer information. The email advises the recipient that direct deposit is the fastest and easiest way to receive their economic stimulus tax rebate. The message contains a hyperlink to a fraudulent form that requests the recipient's personally identifiable information, including bank account information.

More information: <http://www.fbi.gov/pressrel/pressrel08/irsalert050808.htm>

4. 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 June 10th. Check manually too, once every two weeks, to make sure all of the updates have been installed.

More information: <http://www.microsoft.com/athome/security/default.msp#x>

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

More information: <http://www.apple.com/support/downloads/>

iPhones: Must be updated manually:

<http://docs.info.apple.com/article.html?artnum=305744>

5. Security Newsbytes

Safari Carpet Bombing

Serious vulnerabilities in Safari have spawned a troubling attitude from Apple about them. It has been known for years that the Safari browser does not warn users before downloading files to their system. It's a simple trick to get Safari to download a file to the user default file location with no user intervention or notice from the browser. For users who install the Windows version of the Safari browser, that default location is the desktop, so the attacker could fill up your desktop with unsolicited files. The next step is for the Bad Guys to load up your desktop with malware in files named "My Computer"—thus the name "Carpet Bombing" for the attack. On the Mac, the files end up in the Downloads folder. Apple has decided to treat this as a normal product enhancement request and not a security problem.

More information:

http://blogs.pcmag.com/securitywatch/2008/05/safari_carpet_bombing.php

http://www.dhanjani.com/archives/2008/05/safari_carpet_bomb.html

ID Fraud-Prevention Firm LifeLock Hit with Customer Lawsuits

Todd Davis, CEO of LifeLock, has attracted considerable attention and controversy by publicly posting his Social Security number on the company's website and publishing it in ads — all part of an effort to highlight his company's identity theft protection service. But now LifeLock customers in three states are suing Davis and his company for false advertising and deceptive trade practices. Class-action lawsuits filed over the past few weeks in New Jersey, Maryland and West Virginia allege that Tempe, Arizona-based LifeLock has overstated the capabilities of its service and misled its customers. The complaint also asserts that LifeLock actually has failed to protect Davis' identity, saying that his personal information has been misappropriated in at least 20 separate identity-theft incidents.

More information:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=9088538&taxonomyId=82&intsrc=kc_top

38 charged in Romania-US Internet Fraud Bust

International investigators have busted a vast Internet fraud network and charged 38 suspects, most of them Romanians living in the United States. The suspects are accused of using phishing scams to obtain banking information and steal money from the bank, eBay and PayPal accounts of Internet users. The phishing was carried out by Romanian hackers who transmitted the information to US-based accomplices, who used the information in turn to make fake bank cards and withdraw cash from ATM machines.

More information:

http://afp.google.com/article/ALeqM5jsE5wf5AUjUx_IOPpApaDsj1LR_w

California Resident Arrested in Nigerian Fraud Scheme

A 24-year-old man has been arrested by sheriff's detectives, who said he was involved in a \$600,000 Internet fraud scheme with partners in Nigeria. Officials with the sheriff's financial-crimes unit said Kevin Harper of Vista, California was paid to create counterfeit checks, which he mailed to addresses provided by his partners. Authorities said he also received Western Union cash transfers from victims and sent the money to Nigeria.

More information: <http://www.signonsandiego.com/news/northcounty/20080503-9999-1mc3nigeria.html>

Copyright 2008, SANS Institute (www.sans.org).

Editorial Board: Bill Wyman, John York, Barbara Rietveld, Alan Paller. Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.