Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 34

November 16, 2008

IT Security News

It is important to have multiple layers of security protection and not rely on a single solution. Case in point, on Tuesday, November 11, Microsoft released a pair of patches to plug at least four security holes [1]. However one the holes, the Server Message Block (SMB) vulnerability was patched after 7 years in the making [2]. The exploit was first discovered in 2000 and code was published in 2001 [3]. Public tools were readily available to exploit the vulnerability with older machines (Windows 2000, XP, and server 2003) more vulnerable than Vista or Server 2008 [4]. It seems that back in 2001, Microsoft could not fix the security hole without negatively impacting other network-based applications [5]. In explaining why it took so long to fix the bug, a Microsoft person indicated it was only in the last year that it figured out how to fix the flaw without breaking most network-based applications [6]. In general, those responsible for installing security patches still have the dilemma, patch without regression testing knowing exploit tools are in the wild or patch and hope nothing breaks [7]. In other patch news, Apple released 11 security fixes [8].

There is one report of a particular nasty piece of malicious software (malware) that researchers believe may have been in the wild for a year before any anti-virus software detected it (Rustock.c) [9]. In other news, one California Internet provider, where large volumes of Spam and Malware originated from, was cut from the Internet by its upstream provider; thereby temporarily reducing the volume of Internet Spam [10]. Indications are the FBI is investigating the company, McColo, to see if they knowingly aided cyber criminals [11]. With the disconnection of the Internet Service Provider McColo, there was an immediate 40% reduction of Spam across e-mail networks [12]. Overseas, some have reported a Spam decrease of 75% [13].

OMB memorandum, M-07-16 calls for the use of encryption to protect sensitive information. In addressing data protection, Dell and Seagate introduced a new disk laptop security product that uses hardware based encryption to protect disk information [14]. Encryption is often associated with military networking. However, the Defense Sciences Board has referred to the military's network-centric information as its Achilles heel [15]. In the credit card industry, Visa Europe is going to start a 6—12 month test using a card that generates a random number [16]. In other news, Google will be looking for high incidents of searches for flu and report their findings to the CDC [17]. The idea is that more searches probably indicate an outbreak of flu. This is an example of statistical inferencing where information is deduced by frequency use. Consider the same approach looking for combinations of say *bankruptcy* and *company name*. One problem, it is possible to infer an incor-

(Continued on page 2)

Extortion

When we think of extortion, we may visualize some unsavory person in a smoke filled room threatening to release embarrassing information. However, with the Internet and today's technology, cyber extortion has arisen. Case in point, in an attempt to extort an unspecified amount of money, data thieves are threatening to expose millions of patient records of a major pharmacy [1]. In response, St. Louis-based Express Scripts pharmacy, is offering a $1 million reward for information leading to the conviction of the cyber-extortionist [2]. The extortionists have been busy, sending pharmacy clients receiving anonymous letters containing the customer's date of birth and social security number [3]. The letters sent to a small number of clients took place five days after the initial extortion threat [4].

In New Jersey, a former system administrator for New York-

(Continued on page 2)

Inside this issue:

Special points of interest:

- Secretary Paulson reverses direction on TARP, will not purchase troubled assets
- Microsoft SMB Exploit patched after 7 years
- Treasury bank examiner charged with stealing over $500K
- McColo ISP taken down, worldwide Spam decreases 40%—75%

IT Security News

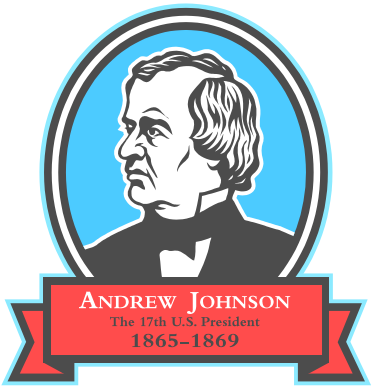
(Continued from page 1)

rect result with disastrous consequences.

With the emphasis on airport security, there are indications that much work remains. For example, the DHS identified Los Angeles International as having poorly guarded computer and telecommunication equipment [18].

1. Krebs, Brian, Washington Post, *Microsoft Patches Four Windows Security Holes*, November 11, 2008.
2. Leffall, Jabulani, Redmond Report, *SMB Exploit Took 7 Years To Fix, Security Pros Say*, November 12, 2008.
3. Rosenberg, Dave, CNet News, *Microsoft takes 7 years to fix security exploit*, November 11, 2008.
4. McMillan, Robert, IDG News service, Microsoft Security Patch Was Seven Years in the Making, November 11, 2008.
5. Leffall, Jabulani, Redmond Report, *Microsoft Faced Big Issues in Fixing SMB Hole*, November 13, 2008.
6. Keizer, Gregg, Computer World, *Microsoft explains seven-year-old patch delay*, November 12, 2008.
7. Swoyer, Stephen, Redmond Report, *IT's Security Dilemma: To Patch or Not To Patch*, November 11, 2008.
8. Vamosi, Robert, CNet News, *Apple updates Safari with 11 security fixes*, November 13, 2008.
9. McMillian, Robert, IDG News Service, *A Sneaky Security Problem, Ignored by the Bad Guys*, November 14, 2008.
10. Keizer, Gregg, Computer world, *Hosting firm shutdown forces botnets to relocate*, November 13, 2008.
11. Menn, Joseph, Los Angeles Times, *Spam traffic plunges after report blames server hosting*, November 14, 2008. company
12. Harris, Scott Duke, San Jose Mercury News, *Cybercrime crusaders shut down shadowy Web hosting operation*, November 13, 2008.
13. Moses, Asher, The Sydney Morning Herald, *Spam drops 75% as major host shut down*, November 14, 2008.
14. Ngo, Doug, CNet News, *Seagate powers self-encrypting Dell PCs*, November 9, 2008.
15. Lipowicz, Alice, FCW, *Defense Science Board warns of cyber problems*, November 7, 2008.
16. Hulme, George, Information Week, *Visa To Test New Credit Card Security Tactic*, November 12, 2008.
17. Kopytoff, Verne, San Francisco Chronicle, *Google.org joins CDC in battle with flu*, November 11, 2008.
18. Weikel, Dan, Los Angeles Times, *Technical security at LAX deemed insufficient*, November 15, 2008.

The goal to strive for is a poor government but a rich people–Andrew Johnson



Extortion

(Continued from page 1)

based mutual fund, Third Avenue Management was detained for trying to extort the company by threatening to have Russian hackers exploit security hole. [5]

1. Kaplan, Dan, SC Magazine, *Crooks threaten to expose data on millions at benefits firm*, November 6, 2008.
2. Kaplan, Dan, SC Magazine, *$1 million reward for arrest of cyberextortionists*, November 12, 2008.
3. Rubenstein, Sarah, The Wall Street Journal, *Express Scripts Says Clients Received Threats*, November 12, 2008.
4. St. Louis Business Journal, *Express Scripts suffers second security breach threat*, November 11, 2008.
5. Efrati, Amir, The Wall Street Journal, *'Crazy' Fired IT Guy Fails in Extortion Plan*, Is Now In Jail, November 11, 2008.

Bogus Rumors

In past newsletters, we discussed computer programs, called algos that operate autonomously (without human intervention), examining news reports and making investing decisions based on these reports. We explored the bogus story on Steve Jobs that drove Apple stock down and the old United Airlines story inadvertently re-released that drove its stock down. So how difficult is it to dupe the press into running a story that later turns out to be bogus? Case in point, recent negative and widely reported news reports regarding Sarah Palin have turned out to be a hoax posted by Martin Eisenstadt, a fictitious person [1]. Two major news organizations, The New York Times and MSNBC were duped into running the story [2].

1. Bauder, David, AP, *MSNBC retracts false Palin story; others duped*, November 13, 2008.
2. Harper, Jennifer, The Washington Times, *Pranksters get the last laugh*, November 14, 2008.

Corporate Bail-Outs

The Government is replacing the original $123 billion AIG bail-out with a new $150 billion package [1]. At the same time, House Speaker Nancy Pelosi and Senate Majority Leader Harry Reid are calling for a bail-out of the big three US auto companies [2]. Meanwhile, the price of GM stock hit a 60-year low [3]. The US auto industry is seeking Government financial relief [4]. The big three are seeking $25 billion in Federal loans [5]. However, it is uncertain what will become of the US automotive industry but there appears to be opposition to a corporate bail-out [6]. One thing to consider is the potential impact to the Government's Pension Benefit Guaranty Corp (PBGC) should there not be a bail-out of the auto industry. For example, the PBGC lost at least $3 billion in investments during its fiscal year with the overall deficit expected between $10 billion and $12 billion [7].

The large consumer electronics chain, Circuit City, has filed for bankruptcy protection [8]. Meanwhile, Fannie Mac reported a $25.3 billion loss [9].

Treasury Secretary Paulson announced a different use for the $700 billion bail-out instead of the original bad assets [10]. Furthermore, there is still no oversight of the Troubled Asset Relief Program (TARP) [11]. Meanwhile, retail sales fell by 2.8% the largest on record [12].

1. Karni, Matthew, et. Al., The Wall street Journal, *U.S. Throws New Lifeline to AIG, Scrapping Original Rescue Deal*, November 10, 2008.
2. Hyde, Justin, Detroit Free Press, *Top Democrats ask Treasury to help automakers survive slump*, November 8, 2008.
3. AP, GM *shares hit 60-year low on cash burn worries*, November 10, 2008.
4. Evanoff, Ted, Indianapolis Star, *Automakers may seek government bailout*, November 8, 2008.
5. Thomas, Ken, AP, *Auto bailout backers offer to cut $25 billion size*, November 15, 2008.
6. Hyde, Justin, and Spangler, Todd, Detroit Free Press, *White House hardens stance on auto loans*, November 15, 2008.
7. Brandon, Emily, U.S. News & world Report, *U.S. Pension Insurance Agency Lost $3 Billion in Stock Investments*, October 22, 2008.
8. Felberbaum, Michael, and Tong, Vinnee, AP, *Circuit City files for bankruptcy protection*, November 10, 2008.
9. Kopecki, David, Bloomberg, *Freddie Asks Treasury for $13.8 Billion After Loss*, November 14, 2008.
10. Crutsinger, Martin, AP, *Paulson says troubled assets will not be purchased*, November 12, 2008.
11. Paley, Amit R., The Washington Post, *Bailout Lacks Oversight Despite Billions Pledged*, November 13, 2008.
12. Chandra, Shobhana, and willis, Bob, Bloomberg, *U.S. Economy: Retail Sales Drop in October by Most on Record* , November 14, 2008.

I have always been afraid of banks–Andrew Jackson

India and China News

Exports in China are starting to moderate indicating the global economic crisis is starting to have an impact [1]. During the third quarter, China's economic growth shrank to 9% from the11.9% rate for 2007 [2]. In response, using its vast currency reserves, China announced a $568 billion stimulus package to keep its economy going strong [3]. At the G-20 economic summit in Washington, China with the largest foreign currency reserves ($2 trillion) and the second largest (Japan with $1 trillion) were asked to provide more support to the International Monetary Fund [4]

Concerned there is a Computer science Ph.D. shortage in India; the IBM Research Laboratory (IRL) is offering students a two year intern with the possibility of joining IRL [5]. Elsewhere, India is expanding its space technology. For example, India is now the 5th country to reach the moon [6]. The Indian probe was successfully crash-landed into the Moon's South pole [7].

In a visible effort to address the growing concern that Chinese dairy products might be contaminate; the Food and Drug Administration (FDA) announced dairy based products from China will be detained until test prove no contaminants [8]. This is an expansion of the current policy enacted when melamine was found in dairy products and now includes products that use dairy products [9].

1. Batson, Andrew, and Shirouzu, Norihiko, Wall street Journal, *Weak Data Point to China Slowdown*, November 11, 2008.
2. Menza, Justin, Business Week/Standard & Poor's Research, *China Bailout*, November 14, 2008.
3. Batson, Andrew, The Wall Street Journal, *China Sets Big Stimulus Plan In Bid to Jump-Start Growth*, November 9, 2008.
4. Lee, Don, Los Angeles Times, *At economic summit, China carries the big stick*, November 14, 2008.
5. Ribeiro, John, Computer World/IDG News Service, *IBM aims to counter researcher shortage in India*, November 6, 2008.
6. The Times of India, Mission Accomplished: India fifth in world to reach moon, November 15, 2008.
7. Rabinowitz, Gavin, AP, *India celebrates planting its flag on moon*, November 15, 2008.
8. Harris, Gardiner, and Martin, Andrew, The New York Times, *F.D.A. Detains Chinese Imports for Testing*, November 13, 2008.
9. Blum, Justin, Bloomberg, *Chinese Milk Products to Be Blocked at U.S. Borders*, November 13, 2008.

To realize that you do not understand is a virtue; Not to realize that you do not understand is a defect–Lao Tzu

Crime

In Georgia, a woman who received over $1 million for her part in a $ multimillion mortgage fraud scheme was sentenced to 11 years in federal prison [1]. Elsewhere in Georgia, a federal jury found a chiropractor guilty in a $3 million health care fraud scheme [2].

In New York, two people were indicted for $9.2 million security fraud [3]. In Virginia, a man pleaded guilty to a $33 million mortgage fraud scheme [4]. In Illinois, a Treasury bank examiner was charged with a number of offenses including 10 counts of forgery, four counts of financial institution fraud, and one count of theft exceeding $500K [5].

1. FBI, *Allen sentenced to more than 11 years in federal prison in mortgage fraud scheme*, November 10, 2008.
2. FBI, *Federal jury finds chiropractor guilty of $3 million health care fraud scam*, November 10, 2008.
3. FBI, *Two principals of Wextrust Capital indicted for securities fraud*, November 10, 2008.
4. FBI, *Fairfax Man Pleads Guilty in $33 Million Mortgage Fraud Case*, November 13, 2008.
5. WBBM (CBS 2), *Treasury Employee Charged With Stealing $500K*, November 13, 2008.