Femtosecond®
www.femto-second.com

In the News

Volume 1 Issue 38

December 14, 2008

Economic News

As investigations continue into the financial crisis, fraud continues to be big news. Case in point, the president of a New York firm was charged with a $50 billion Ponzi fraud scheme [1]. The latest Ponzi scheme is being called the biggest in history [2]. A number of well-known hedge funds that invested at Madoff Investment Securities stand to lose everything [3]. That a multi-billion dollar Ponzi scheme could operate without regulator notice reflects poorly on the money-management industry [4]. In the weeks to come, we should have better idea what the fallout will be on the already troubled economy. How much more white collar crime remains to be detected? Elsewhere in New York, a lawyer was arrested in an alleged $100+ million fraud scheme [5].

Regulators shuttered the 24th bank this year in Georgia, the Haven Trust Bank [6]. In addition, Sanderson State Bank of Texas became the 25th bank closed by regulators [7]. Meanwhile, the Bank of America plans to eliminate up to 35,000 jobs [8]. In a further indication that news organization are struggling, on December 7, the Chicago Tribune was trying to avert bankruptcy [9]. However, on the following Monday (December 8) the newspaper giant filed for Chapter 11 bankruptcy [10]. In Detroit, there are discussions to limit home delivery of newspapers to 3 days per week [11]. In Washington, DC, cost conscience local "channel 9" news will be using one-person crews who will shoot and edit stories [12].

On the positive front, 3 month treasury bills traded for a negative yield for

(Continued on page 2)

IT security

Reports suggest after cyberattacks, the forensics cost is US $5,000–$7,000 per computer [1]. With the high cost of security, some are predicting getting adequate security will be a tough sell especially with the financial crisis diverting funds [2].

There is a rogue program that is billed as a Firefox plug-in but actually steals login information [3]. Obviously, there is a lot of software with security holes yet to be discovered. Moreover, Web based crimeware has reached an all time high [4]. When bad actors find the hole first, honest users suffer. To their credit, vendors continue distributing patches to close security holes. For example, Microsoft released December patches that closed 28 security holes [5]. However, after the patches were released, a new zero-day flaw in the IE version 7.0 [6] was discovered. Furthermore, the security hole also exists in version 6.0 and beta 8.0; the hole is being exploited by hackers; and Microsoft does not have a date for the new patch [7]. This is a challenge for those responsible for ensuring IT security.

In a new voice over IP crime, there is an exploit that allows bad actors to convert compromised user's phones into auto dialers [8]. Meanwhile, in one sample, 82% of web sites in the US have exploitable vulnerabilities [9]. In other news, it is estimated that 60% of the computers used in multiservice businesses are infected [10]. These businesses serve immigrants and personal information is at risk [11].

(Continued on page 2)

Inside this issue:

Special points of interest:

- Man charged in $50 billion Ponzi scheme
- New IE exploit and no patch available
- Chicago Tribune files for bankruptcy
- 3-month Treasury bills trade for a negative yield
- China plans to certify foreign security product imports

Economic News

(Continued from page 1)

the first time ever (This means if you purchased 3 month T-bills, you would lose money) [13]. Elsewhere, Congress is criticizing the Treasury department over their handling of the TARP (the $700 billion bailout) [14]. On the exports front, the trade deficit increased 1.1 % to $57.2 billion [15].

1. Glovin, David, and Scheer, David, Bloomberg, *Madoff Charged in $50 Billion Fraud at Advisory Firm*, December 11, 2008.
2. Walker, David, The Wall street Journal, *Hedge Funds Face Big Losses in Madoff Case*, December 12, 2008.
3. Neumeister, Larry, AP, *Ex-Nasdaq chairman arrested on fraud charge in NYC*, December 12, 2008.
4. Eavis, Peter, The Wall Street Journal, *Letting Madoff Slip Through the Net*, December 12, 2008.
5. Rashbaum, William K., and Cowan, Alison Leigh, The New York Times, *Lawyer Is Accused in Massive Hedge Fund Fraud*, December 8, 2008.
6. Paul, Peralte C., The Atlanta Journal-Constitution, *Haven Trust Bank of Duluth seized after failure*, December 12, 2008.
7. Twaronite, Lisa, Market Watch, *Sanderson State brings total bank failures to 25*, December 12, 2008.
8. Miller, Lisa, NPR, *Thousands Of Employees To Leave Bank Of America*, December 12, 2008.
9. Sorkin, Andrew Ross, The New York Times, *Tribune Hires Advisers to Help Stave Off Bankruptcy*, December 7, 2008.
10. Wilkerson, David B., Market Watch, Tribune *files for Chapter 11 bankruptcy*, December 8, 2008.
11. AP, *Report: Detroit papers likely to cut delivery*, December 12, 2008.
12. Farhi, Paul, Washington Post, *WUSA Moves to One-Person News Crews*, December 12, 2008.
13. Kruger, Daniel, and Eddings, Cordell, Bloomberg, *Treasury Bills Trade at Negative Rates as Haven Demand Surges*, December 9, 2008.
14. Crittenden, Michael R., The wall Street Journal, *Treasury Criticized on Hill Over TARP*, December 11, 2008.
15. Willis, Bob, Bloomberg, *Trade Deficit in U.S. Widens as Exports Decrease*, December 11, 2008.

Early in life I had noticed that no event is ever correctly reported in a newspaper–George Orwell

IT Security

(Continued from page 1)

1. Epstein, Keith, Business week, *U.S. Is Losing Global Cyberwar*, Commission Says, December 7, 2008.
2. Baker, Stephen, Business week, *Cyber-Security: A Hard Sell*, December 9, 2008.
3. Miller, Chuck, SC Magazine, *Malware posing as Firefox plugin steals login information*, December 5, 2008
4. Cnet, *Web site-based crimeware hits all-time high*, December 10, 2008.
5. Krebs, Brian, The Washington Post, *Microsoft Plugs at Least 28 Security Holes*, December 9, 2008.
6. Leffall, Jabulani, Government Computer News, *Flaw found in Internet Explorer 7*, December 11, 2008.
7. Keizer, Gregg, Computer World), *Microsoft confirms that all versions of IE have critical new bug*, December 12, 2008.
8. Goodwin, Jacob, Government Security News, *FBI warns against telephone 'vishing' attacks*, December 9, 2008.
9. Jackson, William, Government Computer News, *The Web is more dangerous, and U.S. is biggest culprit*, December 10, 2008.
10. Claburn, Thomas, Information Week, *Poor Computer Security Putting Immigrant Data At Risk*, December 12, 2008.
11. Government Technology, *Multi-Year Security Assessment of Business Services for U.S. Immigrants*, December 12, 2008.

Auto Industry

The long debated auto industry bailout loan died in the Senate [1]. However, there are suggestions that the TARP fund may be used to aid the auto industry [2]. The plan calls for $14 billion in short term loans [3]. The emergency loan would only go to Chrysler and GM as Ford has sufficient funds [4]. One estimate suggests that a GM bankruptcy could result in 2.5 million job losses [5]. While the discussion continues, the US unemployment claims hit a 26-year high [6].

1. Herszenhorn, David M., The New York Times, *Senate Drops Automaker Bailout Bid*, December 12, 2008.
2. Reuters/Washington Post, *US-Business Summary*, December 13, 2008.
3. Coile, Zachary, San Francisco Chronicle, *White House offers lifeline to automakers*, December 13, 2008.
4. Puzzanghera, Jim, and Bensinger, Ken, Chicago Tribune, *White House prepares to give aid to automakers*, December 13, 2008.
5. McKee, Michael, Bloomberg, *GM, Chrysler Bankruptcies Would Cause Turmoil for U.S. Economy*, December 12, 2008.
6. Clifford, Catherine, CNN Money, *Jobless claims at 26-year high*, December 11, 2008.

Cyberwarfare

We have seen numerous reports of hacker attacks and to some extent organized cyberwarfare capabilities. For example, two years ago, China downloaded between 10 and 20 terabytes of Pentagon data [1]. However, to better understand what we can expect it is worth examining some lessons from the Middle-East.

After the Israel Defense Forces (IDF) entered the Gaza in 2006, pro-Palestinian hackers shut down approximately 700 Israel web domains [2]. Having the capability to shut down domains certainly can be disruptive but actual attacks against military targets are the gold standard.

Consider the example when Israel bombed a target in Syria believed to be a clandestine nuclear facility [3]. During the attack, two state of the art Russian built radar systems failed to detect the Israel attack leading to speculation as to what type of cyberwarfare capability was used [4]. This was a clear demonstration how radar could be turned off long enough to conduct a bombing operation using cyberwarfare techniques as opposed to traditional jamming [5].

Clearly, the value of cyberwarfare is emerging as a viable component of military warfare. But how does one learn enough about existing security controls in order to develop approaches to circumvent them? Perhaps the boldest approach to date can be seen by the Chinese Government. Starting May 1, vendors of 13 security products must have their products certified before they can be sold [6]. The very same products used to protect American commercial and Government information technology will be completely explained to our potential adversary. Companies that build their security into their products will likely be required to expose all internals to the Chinese in order to tap that market. Another consequence that could have far greater ramifications is this new knowledge could allow Chinese industry to build their own security export industry [7]. Imagine Chinese manufactured security appliances and software protecting America's critical infrastructure.

1. Kingsbury, Alex, US News and World Report, *When Do Online Attacks Cross the Line Into Cyberwar?*, December 9, 2008.
2. Stoil, Rebecca Anna, and Goldstein, James, Jerusalem Post, *One if by land, two if by modem*, June 28, 2006.
3. AP/CNN, *Report: Israeli airstrike targeted Syrian nuclear reactor*, October 15, 2007.
4. Fulghum, David A., and Barrie, Douglas, ABC News, *Israel used electronic attack in air strike against Syrian mystery target*, October 8, 2008.
5. Fulghum, David A., Aviation week and Space Technology, *Network Attack Gets Tougher*, January 21, 2008.
6. CBC (Toronto), *China to demand details of security technology from foreign companies*, December 8, 2008.
7. Las Vegas Sun/AP, *China irks US with computer security review rules*, December 8, 2008.

Newspaper editors are men who separate the wheat from the chaff, and then print the chaff–Adlai E. Stevenson

China News

Having an advanced cyber-attack capability provides the ability to punish countries that oppose your will. Case in point, after the French president met with the Dalai Lama, a critic of China, the French embassy in Beijing was subjected to a cyber-attack [1]. Elsewhere, a Chinese team inadvertently release code to exploit a security hole in unpatched versions of Internet Explorer 7.0 potentially placing millions of computers at risk [2].

Certain to raise eyebrows in Congress, for October the US reached a new record trade deficit with China of $28 billion [3]. This works out to roughly 49% of the US trade deficit is with China. In further non-cooperation, to help increase its trade, China plans to weaken its currency relative to the dollar [4]. This is trade protectionism that will make Chinese goods cheaper and American goods more expensive. In other trade related news, China has a plan to require foreign computer security technology examination and approval by the Chinese government before it can be imported [5]. So if a security vendor wants to sell products in China it must divulge how their product works. Given these security products are used to protect US resources; this should be a windfall for Chinese cyber-attack capabilities.

1. Spencer, Richard, The Telegraph (UK), *French embassy in Beijing 'under cyber-attack' after Nicolas Sarkozy meeting with Dalai Lama*, December 11, 2008.
2. PC World, *Chinese Team Mistakenly Released Unpatched IE7 Exploit*, December 11, 2008.
3. Crutsinger, Martin, AP, *Trade deficit rises unexpectedly in October*, December 11, 2008.
4. Oliver, Chris, Market Watch, *China's yuan set to weaken for six months*, December 11, 2008.
5. AP, *China irks US with computer security review rules*, December 8, 2008.

Four hostile newspapers are more to be feared than a thousand bayonets– Napoleon Bonaparte

Crime

An Oregon man pleaded guilty to defrauding Cisco out of $7.9 million for false parts claims [1]. In Florida, a man pleaded guilty for his part in fraudulent schemes totaling over $11 million [2]. In California, a woman pleaded guilty to $1.7 million in fraudulent real estate investments [3]. Elsewhere in California, a former CEO was sentenced to 97 months in Federal prison for his fraudulent schemes that shareholders claim cost over $3 billion [4]. In New York, a former FBI supervisor pleaded guilty to criminally accessing an FBI database for personal gain [5]. In Idaho, a builder pleaded guilty to illegally helping obtain $20 million in construction loans [6]. Mortgage fraud is best described by U.S. Attorney McGregor Scott who asserts there is immense criminal fraud involved in the financial crisis [7].

In efforts to fight computer crime, many tools are available. For example, the VOOM Shadow 2 is a hardware tool designed to preserve evidence while booting and reading the disk without first copying [8]. Another tool is a LoJack security system for the MacBook Pro that takes pictures of the person trying to use the computer and if connected to the Internet, sends the location information [9].

1. AP, *Man pleads guilty in $7.9 million fraud scheme*, December 11, 2008.
2. FBI, *Pembroke Pines man pleads guilty to massive fraudulent schemes*, December 10, 2008.
3. FBI, *Former mortgage lender pleads guilty to fraud in connection with real estate investment scheme*, December 11, 2008.
4. FBI, *Former Peregrine Systems, Inc. CEO to Serve 97 Months in Federal Prison*, December 11, 2008.
5. FBI, *Former Federal Bureau of Investigation (FBI) Supervisory Special Agent Pleads Guilty to Criminally Accessing FBI Database*, December 8, 2008.
6. AP, *Builder last of 5 to plead guilty in ID bank fraud*, December 12, 2008.
7. Thompson, Don, The Seattle Times/AP, *On the trail of mortgage fraud*, December 13, 2008.
8. Rutherford, Mark, CNet, *Investigators now crack crime computers on the spot*, December 11, 2008.
9. KRNV, *High-tech computer security gives police lead in crime*, December 11, 2008.