

IN THE NEWS

MARCH 14, 2010

Economic News

The economic recovery is still weak as demonstrated by high unemployment. For example, for the 25th time in the past 26 months, non-farm payrolls fell; this time by 36,000 jobs [1]. For the week ending February 27, the number of first time job claims fell to 469,000 [2]. During the week ending March 6, the first time unemployment number fell again to 462,000 [3].

In past newsletters, we have highlighted the role of automatic computer trading (algorithms) triggered to trade on news posts. The impact of trades hit the largest banks. Case in point, the CEO of Citigroup testified before a Congressional oversight committee that the Citi's problems were the result of short selling, not the health of the bank [4]. Elsewhere a report on the Lehman fall,

prepared at a cost of \$38.4 million so far, was released by the Chicago based law firm Jenner & Block LLP [5]. The report indicates that Lehman used an accounting technique, Repos, in London to inflate the available assets [6]. In looking over the report, it shows how dependent Lehman was on assets and the difficulty of identifying the root causes. Many of the transactions were for the same amount during the same day suggesting the role in volume computer transfers. By using the London repo rule, computer algorithms could quickly calculate what was needed. Interestingly, in instances where the investigator looked for fraud, no smoking gun could be found. This suggests a larger story yet to be uncovered.

(Continued on page 2)



IT Security

Readers may recall the year 2000 (Y2K) bug that was supposed to cause havoc when the computer date changed to January 1, 2000. Originally, security people pointed out the problem and it became a cottage industry for non-security personnel. Now it appears a leap year bug shut down Sony Play Station games in mass [1]. Meanwhile, Microsoft is working on a fix for yet another

Internet Explorer vulnerability; unfortunately the exploit was published on the web [2]. This is an example where hackers have the ability to exploit vulnerabilities and there is no fix available to correct the problem. All a bad actor needs to do is to compromise a system, install multiple back doors, and then it no longer matters when the vulnerability is fixed; the hacker owns the

system.

The transportation industry is increasingly using GPS for determining location. However, the GPS is becoming more vulnerable to ground based hacker attacks [3].

One of the first things cyber attackers do is to scope out or probe the environment before launching the attack. Case in point, the Chinese attacks

(Continued on page 2)

Inside this issue:

Counterfeit Chips	3
World News	4
Crime	4

Special points of interest:

- Bank closings so far this year exceed all of 2008 and 2009
- Chinese cyber-attack on Google targeted company source code
- 30 banks shuttered this year

Economic News

(Continued from page 1)

Meanwhile, regulators continued closing financial institutions. So far, 30 banks have been closed this year; more than 2007 and 2008 combined. On March 4, four banks were closed: 23) Sun America Bank in Florida; 24) Bank of Illinois; 25) Waterfield Bank in Maryland; and 26) Centennial Bank in Utah [7]. In an unusual closing, regulators shuttered the 27th financial institution, Liberty-Pointe Bank in New York on March 11 [8]. Resuming bank closing on March 12, three more were closed: 28) Park Avenue Bank; 29) Old Southern Bank in Orlando, Florida; and 30) Statewide Bank in Covington, Louisiana [9].

1. Nutting, Rex, Market Watch, *Payrolls fall by 36,000; U.S. jobless rate steady at 9.7%*, March 5, 2010
2. Rugaber, Christopher S, AP, *Jobless claims drop, retail sales climb*, February 4, 2010.
3. Bartash, Jeffry, Market Watch, *Weekly jobless claims dip 6,000 to 462,000*, March 11, 2010.
4. Braithwaite, Tom, and Rappeport, Alan, Financial Times, *Pandit blames Citi's woes on short selling*, March 4, 2010.
5. Efrati, Amir, Wall Street Journal, *Probe Yields Windfall For Legal Examiner*, March 11, 2010.
6. Craig, Susanne, and Spector, Mike, Wall Street Journal, *Repos Played a Key Role in Lehman's Demise*, March 13, 2010.
7. Palmer, Doug, Reuters, *Regulators close banks in four states*, March 5, 2010.
8. McGeehan, Patrick, New York Times, *State Regulators Shut Down a City Bank, LibertyPointe*, March 12, 2010.
9. Kell, John, Wall Street Journal, *Three Failed Banks Closed Friday; 2010 Total At 30*, March 12, 2010.

*To talk much and arrive
nowhere is the same as
climbing a tree to catch a
fish—Chinese Proverb*

(Continued from page 1)

against Google focused on a limited number of machines that kept source code [4]. Stealing source code suggests the Chinese are looking for ways to compromise Google in the future. What's more, the last attack was so good, China stated it would punish the hackers if it could be shown who did it [5]. Of course if Google could show China how it determined who launched the attack; China could use this information to improve its next attack. Often considered one of the best privacy protected institu-

tions, Swiss banks, have been shown to be vulnerable. Case in point, information on approximately 24,000 Swiss accounts has been stolen [6].

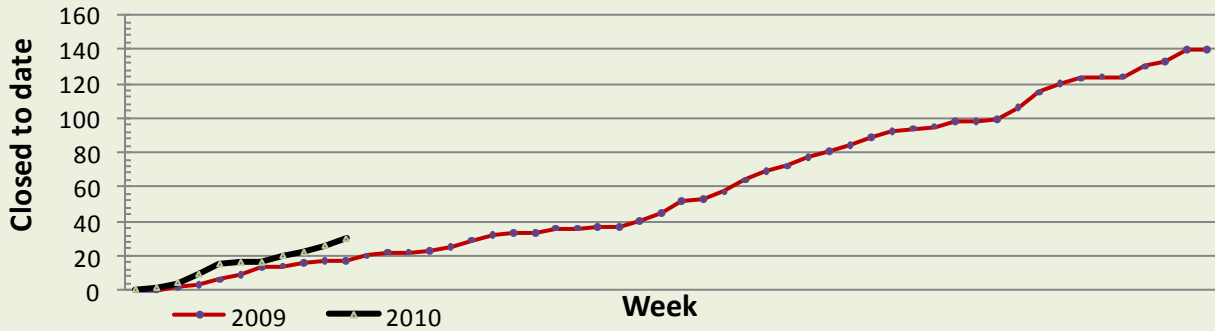
1. Nystedt, Dan, IDG News Service, *Sony Blames Leap Year Glitch for PlayStation Troubles*, March 2, 2010.
2. Mills, Elinor, Cnet News, *Microsoft races to plug IE hole after exploit code released*, March 12, 2010.
3. Palmer, Jason, BBC News, *GPS vulnerable to hacker attacks*, February 23, 2010.
4. Finkle, Jim, Reuters,

Google China hackers stole source code - researcher, March 3, 2010.

5. Blanchard, Ben, Reuters, *China to punish hackers, says no Google complaint*, March 6, 2010.
6. Jordans, Frank, AP, *HSBC: data on 24,000 Swiss account holders stolen*, March 11, 2010.

IT Security

Financial Institution Closures as of 3/14/2010



Counterfeit Chips

Counterfeit hardware has once again found its way into the news. Case in point, bogus Intel CPU's (Core 17 Processors) were discovered in circulation [1]. The fake chips entered the system from the distributor Newegg [2]. In turn, the devices were allegedly supplied to Newegg by Ipex Infotech out of Fremont, California [3]. The fake Intel devices included a number of tell-tale problems including the misspelling "socket" as "sochet" on the device box [4].

This is not the first time counterfeit chips found their way into the marketplace. For

example, last year a man pleaded guilty to selling thousands of counterfeit chips imported from China to the Naval Sea Systems Command, the Washington, D.C. [5]. This illustrates how weaknesses in the parts supply chain could be used to place rogue chips into America's critical infrastructure. A single rogue chip in a critical system could be catastrophic.

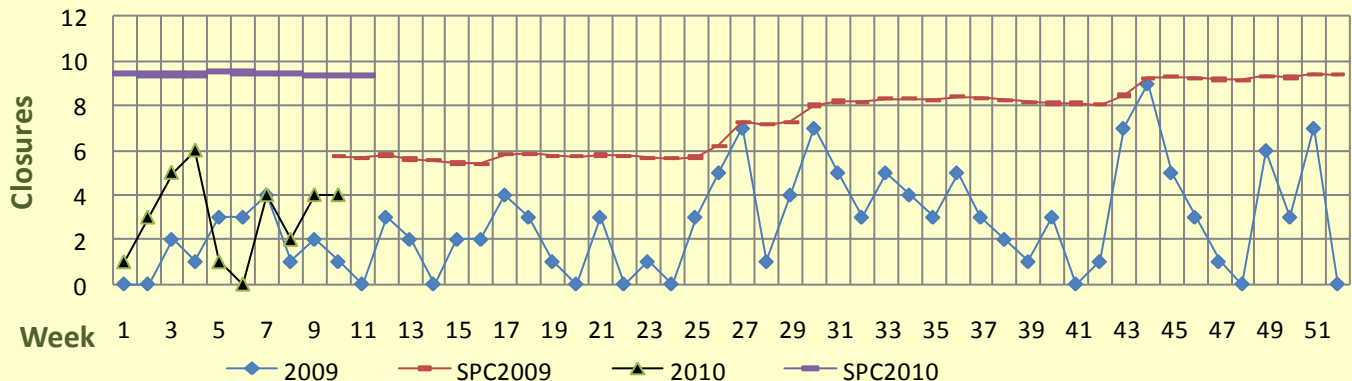
1. Bradley, Tony, PC World, *Four Reasons to Beware Fake Intel CPU's*, March 8, 2010.
2. Gonslaves, Antone, Information week, *Newegg Axes Supplier Over Fake*

Intel Chips, March 9, 2010.

3. Campbell, Scott, and Poeter, Damon, Channel Web, *Supplier Of Fake Intel Chips Denies Being Original Source*, March 9, 2010.
4. Burt, Jeffrey, eWeek, *Newegg Fires Supplier IPEX in Fake Intel Chip Flap*, March 9, 2010.
5. McMillian, Robert, IDG News Services, *Man pleads guilty to selling fake chips to US Navy*, November 25, 2009.

*Always take hold of things
by the smooth handle –
Alexander Hamilton*

Failed Banks Vs SPC Threshold 3/14/2010



World News

At least one Chinese army officer is suggesting that China should use its acquired wealth to become the world's dominant military power [1]. Meanwhile, China announced it will increase its defense force by only 7.5%; exceeding the budgets of Russia, France, and the U.K. [2]. At the same time, China will not approve any sanctions against Iran that would slow Chinese oil supplies and investments [3]. To put this in context, China needs Iran's oil so it can manufacture subsidized goods for export to the U.S.; thereby increasing American unemployment. In chorus, China's artificially low currency helped it grow exports by 46% during February [4].

In its role as a currency manipulator, China continues to draw jobs away from the U.S. thereby keeping \$billions out

of the tax collecting system. It should come as no surprise that China resists suggestions to change the current approach. Case in point, the People's Bank of China Vice Governor Su Ning advised the U.S. not to make the Chinese currency manipulation a political issue [5].

While the U.S. is refining its energy policy, other countries continue to expand their nuclear power generating capability. For example, Russia will build 12 nuclear power plants for India [6]. Additionally, India is purchasing \$7 billion in military sales from Russia [7].

1. Buckley, Chris, Reuters, *China PLA officer urges challenging U.S. dominance*, February 28, 2010.
2. Fairclough, Gordon, Wall Street Journal, *China*

Raises Defense Spending 7.5%, March 4, 2010.

3. Graham-Harrison, Emma, Reuters, *China says Iran sanctions no cure*, March 7, 2010.
4. Pierson, David, Los Angeles Times, *China exports leap 46% in February*, March 10, 2010.
5. Wang, Aileen, Reuters, *Leave yuan to us, China tells Obama*, March 12, 2010.
6. AFP, *Russia to build 12 nuclear reactors in India*, March 12, 2010.
7. Magnier, Mark, Los Angeles Times, *India embraces Russia arms*, March 13, 2010.

*The soldier, above all other
people, prays for peace, for he
must suffer and bear the
deepest wounds and scars of
war—Douglas MacArthur*

As we consider the topic of crime, it's interesting to note the futility of armed robbery. Consider in Philadelphia, a man was sentenced to 8 years in prison for robbing and M&T Bank of \$950 [1]. The risk to the criminal is high and the monetary return is low. Yet the high dollar white collar crime relentlessly continues. Meanwhile the losses due to Internet scams doubled during 2009 [2]. For every electronic robbery, what is the likelihood of getting caught? In past newsletters we have seen sufficient reports of Chinese and Russian attacks to our financial systems with a very low arrest rate. In summary, we are extremely good at capturing armed robbers while struggling with elec-

tronic robbery.

The Securities and Exchange Commission charged *America's Prophet* with a \$6 million fraud scheme [3]. In Michigan, a member of the Winans gospel-music family was charged in a multi-million dollar Ponzi fraud scheme [4]. In Florida, a couple was charged with operating a \$135 million Ponzi scheme [5]. Furthermore, four men were charged with a \$25 million on-line sporting events ticket fraud [6].

1. FBI, *Bank Robber Sentenced to Eight Years for \$950 Haul*, March 5, 2010.
2. Godinez, Victor, Dallas Morning News, *Cost of Internet scams more than*

doubled in '09, March 13, 2010.

3. McCool, Grant, Reuters, *SEC accuses "America's Prophet" of investor fraud*, March 4, 2010.
4. Karoub, Feff, AP, *Winans family member accused of Ponzi scheme*, March 4, 2010.
5. Patel, Yogita, Wall Street Journal, *SEC Charges Couple in Florida Ponzi Case*, March 4, 2010.
6. Mills, Elinor, Cnet News, *Four men charged in computerized online ticket scam*, March 1, 2010.