Femtosecond®
www.femto-second.com

In the News

Volume 2 Issue 4

January 25, 2009

IT Security

Hardly a week passes without another privacy breach being reported. Last week, came the report, over 100 million credit and debit card transactions were compromised at Heartland Payment Systems [1]. Apparently spy software stole payment card data as it passed through the company's private network [2]. Heartland first became aware of the problem when Visa and MasterCard reported suspicious activity surrounding processed card transactions [3]. The company then hired a forensic team and alerted law enforcement [4]. The malicious software (malware) was described as significantly more sophisticated than commonly downloaded programs [5]. The company claims to use encryption but the malware resided at the point where the transaction information remains in unencrypted format [6]. Heartland offered no clues to when the breach occurred, how long the breach went undetected, or how many cards might have been compromised [7]. The president and CFO for Heartland Payment Systems, Robert Baldwin, Jr., indicates the first alert came in October and they do not know how the software got onto the system [8]. It should be noted that the breached system was Payment Card Industry Data Security Standard (PCI-DSS)-audited and certified [9]. This illustrates the weakness where PCI-DSS does not require encryption inside a private network [10]. Understandably, the lack of details is causing angst in the payment processing industry [11].

Recent malware has included code to prevent infections in certain countries. For example, the Conflictor avoids Ukraine and Swizzor avoids Russian machines [12]. Regarding the Conflictor worm, one sample showed 6% of machines infected making this a malware epidemic [13]. What's more, the U.S. Computer Emergency Readiness Team (US-CERT) assets, Microsoft's advice to turn off the autorun feature as inadequate [14]. The malware looks like a multi-stage infection; however we don't know what the next stage is [15].

(Continued on page 2)

Economic News

The big banks continue to search for cash. For example, after investing $15 billion in its Japanese business, Citigroup is looking to sell some of its units [1]. Furthermore, the new Citigroup Chairman, Richard Parsons, acknowledged bank lending was down due to balance sheet issues [2]. To raise cash, Citi sold $12 billion in FDIC insured notes [3].

Meanwhile, regulators shuttered bank number 3, the1st Centennial in California [4]. The impact to the FDIC deposit insurance fund, which had $34.6 billion as of September 30, is expected to cost $227 million [5].

Readers may recall the Government urged Bank of America (BofA) to purchase Merrill Lynch [4]. Now there is an investigation by the New York Attorney General to determine if Merrill awarded large, secret, last-minute bonuses to employees days before the BofA takeover [5]. Merrill Lynch moved up year-end bonuses to December, just prior to the company acquisition by BofA [6]. The former CEO of Merrill, John Thain, was ousted from BofA following an unexpected $15.31 billion fourth-quarter loss [7]. What is more, before leaving, Thain spent $1.2 million to have his office redecorated [8].

The New York Times secured a $250 million loan paying 14% from Mexican billionaire, Carlos Slim [8]. In other efforts to raise money, the NY Times is negotiating to sell several floors in its headquarters office building [9].

1. Doland, David, Reuters

(Continued on page 2)

Inside this issue:

Special points of interest:

- 100 million credit and debit card transaction breach at Heartland Payment Systems
- 6% of computers infected with Conflictor malware
- 1st Centennial becomes third bank closed in 2009
- Vandals hack into Wired Magazine web site and post bogus Steve Jobs story

IT Security

(Continued from page 1)

The former SEC Chairman Christopher Cox blamed the failure of Bear Sterns on false rumors. Accordingly, whenever bogus news is published on a news site, this becomes newsworthy. Last week, hackers posted a bogus story about Steve Jobs on the Wired Magazine web page [16]. We expect to see future stock manipulation using hackers posting bogus stories.

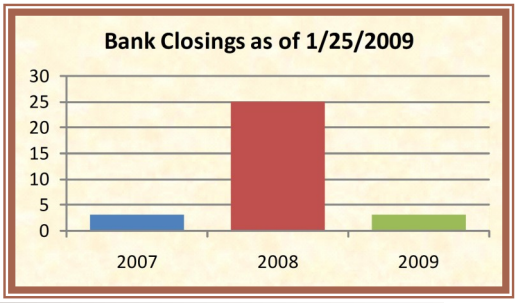
1. Krebs, Brian, Washington Post, *Payment Processor Breach May Be Largest Ever*, January 20, 2009.
2. Larking, Erik, PC World, *Massive Theft of Credit Card Numbers Reported*, January 20, 2009.
3. Messmer, Ellen, Network World, *Debit-card processor claims data breach part of global fraud operation*, January 20, 2009.
4. Kaplan, Dan, SC Magazine, *Payment processor discloses potential monster breach*, January 20, 2009.
5. Worthen, Ben, Wall street Journal, Card Data Breached, Firm Says, January 20, 2009.
6. Dash, Eric, and Stone, Brad, New York Times, *Credit Card Processor Says Some Data Was Stolen*, January 20, 2009.
7. Vijayan, Jaikumar, Computer World, *Heartland data breach could be bigger than TJX's*, January 20, 2009.
8. Krebs, Brian, Washington Post, *Firm Reports Massive Data Breach From Credit, Debit Transactions*, January 21, 2009.
9. Haskins, Walaika, Tech News World, *Heartland Bleeds Data, Potential Victims Could Number Millions*, January 21, 2009.
10. Messmer, Ellen, Network World, *Heartland breach raises questions about PCI standard's effectiveness*, January 22, 2009.
11. Vijayan, Jaikumar, Computer World, *Heartland data breach sparks security concerns in payment industry*, January 22, 2009.
12. Moscaritolo, Angela, SC Magazine, *Malware purposely not infecting machines in certain countries*, January 16, 2009.
13. Albanesius, Chloe, PC Magazine, *Conficker/Downadup Worm Dubbed 'Epidemic'*, January 21, 2009.
14. Keizer, Gregg, Computer World, *Microsoft's advice on Downadup leaves users open to attack, says US-CERT*, January 21, 2009.
15. Markoff, John, New York Times, *Worm Infects Millions of Computers Worldwide*, January 22, 2009.
16. Fox News, *Pranksters Hack Into Web Site, Start Rumor Steve Jobs Died*, January 23, 2009.

The big thieves hang the little ones—Czech Proverb

Economic News

(Continued from page 1)

(UK), *Citi sale could be game-changer in Japan*, January 19, 2009.
2. Nye, Karen, BBC News, *Citi wants further help for banks*, January 22, 2009.
3. Coppola, Gabrielle, Bloomberg, *Citigroup Raises $12 Billion in FDIC-Backed Bond Sale*, January 23, 2009.
4. Reckard, E. Scott, *1st Centennial Bank in Redlands is shut by state regulator*, Los Angeles Times, January 24, 2009.
5. Bloomberg News, *Third Bank Is Seized This Year*, January 23, 2009.
6. Cox, Rob, New York Times, *A History Lesson With Merrill Deal*, January 22, 2009.
7. Landy, Heather, Washington Post, *Former Merrill Chief Is Out at Bank of America*, January 22, 2009.
8. Bernard, Stephen, and Augstums, Ieva M., AP, *Thain resigns from Bank of America*, January 22, 2009.
9. Comlay, Elinor, Reuters, *Thain: Unlikely poster boy in Wall St blame game*, January 23, 2009.
10. New York Times, *Thain's Office Overhaul Said to Cost $1.2 Million*, January 22, 2009.
11. AP, *NY Times agrees to financing deal with billionaire*, January 20, 2009.
12. AP, *NY Times negotiating sale for part of its building*, January 23, 2009.



Basement Cyberwar

The U.S. military is trying to understand the full implications of cyberwar and how to utilize its capabilities [1]. Typically, large Government programs involve large budgets, large teams, and closed door development. This may be an effective mythology for large systems, however, large teams often lose sight of the bigger picture. A smaller team may provide a better return on investment.

Consider the UNIX operating system, developed by two people, Dennis Ritchie and Ken Thompson [2]. Few would question the importance of the UNIX operating system. Then in 1984, Ken Thompson shocked the computer world by demonstrating the ease of creating a Trojan horse with the C language compiler that would allow Ken to log into any compromised program [3]. That is, any program complied using the exploited compiler would allow a nefarious login.

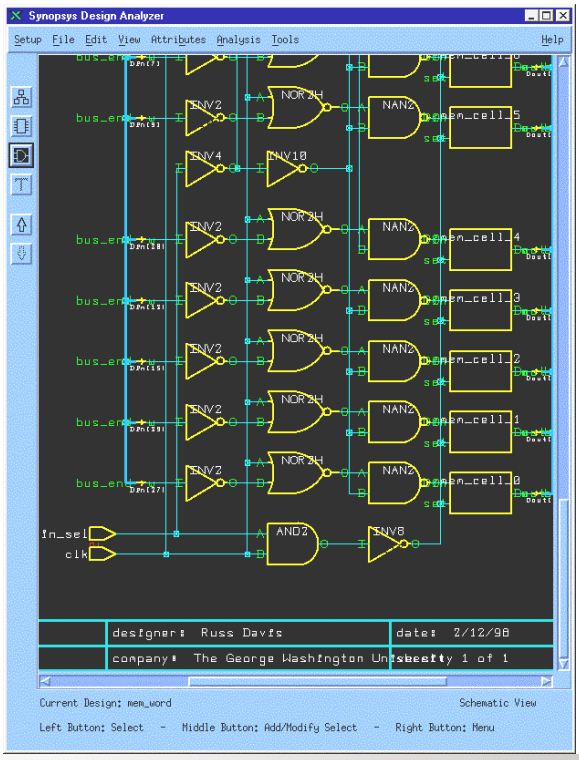
Today's software consumes vast quantities of space allowing optimized malicious software (malware) ample room to hide. Programs written in more terse languages, such as assembly, can result in faster programs requiring a fraction of the space [4]. To be sure, the malware version of a program could be built to execute much faster than the legitimate version. In such a case, users might restore the bogus backup because of the improved performance. Exploits are possible due to program complexity, lack of quality in new products, and the rush to quickly get products in the market.

Software exploits are not exclusive; consider the ramifications of a hardware exploit. In most cases, the cost to fix a hardware bug may simply be too expensive. If a bad actor discovers a bug first, he or she may be able to introduce a killer exploit. The bulk of processors today are made by Intel. Bugs discovered in hardware are not uncommon. When Intel introduced the 80386 processor, a bug was discovered in 1987 [5]. Likewise, the 80486 had a bug discovered in 1989 [6]. Furthermore, the Pentium had a bug discovered in 1994 [7].

A more serious problem would be the deliberate introduction of a Trojan horse into a chip. Today integrated circuits are but an instance of software developed tools. The picture shown is a screen scrape from a synthesis tool. If a bad actor could replicate an exploit similar to what Ken Thompson demonstrated with the C compiler to hardware generating tools, then the damage would be irreparable .

1. Fulghum, David A., Aviation Week and Space Technology, *Cyberwar Takes Shape*, January 19, 2009.
2. Science Daily, *Bell Labs Luminaries Dennis Ritchie and Ken Thompson to Receive National Medal of Technology*, December 8, 1999.
3. Thompson, Ken, Communications of the ACM, *Reflections on Trusting Trust*, August, 1984.
4. Davis, Russell, Proceedings of the Fourth Aerospace Computer security Applications Conference, *Exploring Computer Viruses, December*, 1988.
5. San Jose Mercury News, *Intel discovers a bug in its new 80386 chip*, April 11, 1987.
6. San Jose Mercury News, *Intel stops making 80486*, October 27, 1989.
7. Gillooly, Brian, and Needle, David, Information Week, *PC vendors say sales haven't been affected*, December 9, 1994.

A thief passes for a gentleman when stealing has made him rich–Dutch Proverb



Asian News

Tension between India and Pakistan remains high. Highlighting the anxiety, in a show of force, India launched a new nuclear capable supersonic cruise missile [1]. Adding to the stress Indian External Affairs Minister Pranab Mukherjee claims Pakistan is still sponsoring terrorism and must be punished [2].

The world recession is starting to slow China's economic growth. For the fourth quarter, China's growth slowed to 6.8%, the lowest in 7 years [3]. International relations between China and the U.S. could be headed for rough times. Case in point, Timothy F. Geithner's told the Senate Finance Committee, Beijing is manipulating its currency and the new administration will act aggressively [4]. This is the highest level Government official to strongly implicate China in currency manipulation [5]. In response to the allegation, China denied it is manipulating its currency [6]. In addition, Chinese ministers cautioned Secretary of State, Hillary Clinton, to handle ties with China carefully [7].

1. Laurence, Jeremy, Reuters, *India tests missile amid tensions with Pakistan*, January 20, 2009.
2. UPI, *India: Pakistan must be brought to justice*, January 21, 2009.
3. Hamlin, Kevin, and Yanping, Li, Bloomberg, *China's GDP Growth Slowed to 6.8% in Fourth Quarter*, January 22, 2009.
4. Montgomery, Lori, and Faiola, Anthony, Washington Post, *Geithner Says China Manipulates Its Currency*, January 23, 2009.
5. Jianxin, Lum, and Rabinovitch, Simon, Reuters, China notes U.S. yuan charge, to hold anger in check, January 23, 2009.
6. AFP, *China tells Obama's Treasury pick it is not manipulating currency*, January 23, 2009.
7. Maidment, Paul, Forbes, China, *New U.S. Administration Make Yuan First Row*, January 23, 2009.

Success is how high you bounce when you hit bottom–George S. Patton

Crime Report

The Florida Fund manager who disappeared was charged by the SEC with fraud [1]. The 500+ investors, collectively owed a $50 million payout, were informed funds were empty [2]. Elsewhere in Florida, an ex-bank employee was charged with defrauding foreign customers out of $11 million [3].

Fraud exceeding $1 million continues to make the news. For example, a Missouri homebuilder was charged with defrauding subcontractors out of $10 million [4]. In California, a man was arrested for nine counts of bank fraud and nine counts of wire fraud where $1.7 million in client funds were misappropriated [5]. In Connecticut, a developer was indicted for a $6 million bank fraud scheme [6]. In Massachusetts, a securities broker was accused of a $2 million fraud by selling clients phony securities [7]. In Michigan, four people were charged by the state Attorney General in a $1 million mortgage fraud [8]. In Pennsylvania, a man was charged with running a $50 million Ponzi scheme [9].

While $1 million fraud schemes make the news, there are a number of smaller cases that are increasing in number. Case in point, in Tarrant country, Texas, where mortgage fraud once was a rarity, $42 million in new cases are flooding the legal system [10].

1. Loney, Jim, Reuters, *U.S. charges missing Florida fund manager with fraud*, January 21, 2009.
2. Gordon, Marcy, AP, *SEC charges missing money manager Nadel with fraud*, January 21, 2009.
3. AP, *Ex-bank employee in Florida charged with fraud*, January 21, 2009.
4. AP, *Missouri homebuilder accused in fraud scheme*, January 23, 2009.
5. FBI, *Former South Bay Financial advisor arrested for fraud*, January 20, 2009.
6. AP, *Developer indicted on bank fraud charges*, January 23, 2009.
7. AP, Galvin seeks to suspend broker in fraud case, January 23, 2009.
8. PRNewswire, *Four Charged in Million Dollar Mortgage Fraud*, January 21, 2009.
9. FBI, *Delaware County Man Charged in Large Scale Investment Fraud*, January 23, 2009.
10. McDonald, Melody, Start Telegram (Fort Worth), *Mortgage-fraud cases are flooding into Tarrant County district attorney's office*, January 18, 2009.