ISSN:2229-6247

World financial crisis and cybercrime

Bashar Matarneh, Dr.Hazem .k.shehadeh

Department of Business Administration, Delmon University, P.O. Box 2469,Exhibition Avenue Manama, Kingdom of Bahrain

Abstract

This paper considers how information and communications technologies (ICT) used by organized crime groups in world financial crises. It also raises broader analysis using up-to-date statics about the relationship between cybercrime and world financial crises and how the financial crises support a good environment for spam, scam, …, etc. because of the inconsistency and lack of information in addition to panic around the world. Appropriate recommendations suggested in this regard.

Keywords: *Cybercrime, world financial crises, spam, botnets, organized-crime*

1. Introduction

With the credit crisis affecting consumers and businesses, spammers and cyber-criminals sought to take advantage of the resulting panic and uncertainty. To capitalize, spammers increased the number of finance-related emails, including phishing attacks targeting banks and credit unions, lottery scams, loan and job offers and other financial enticements [1][18][19].

In late 2008, speculation about the future of many global banks ensued. Phishers exploited this uncertainty by increasing the volume of phishing emails targeting banks involved in proposed mergers and acquisitions, making reference to news of anticipated takeovers in their messages. Scammers swiftly updated their templates to reference other banks as news of which banks were involved in mergers changed.

Security researchers have issued a security alert that reveals a direct correlation between the recent stock market volatility and the growth of new threats.

According to the global IT security vendor, the two are tied together much more closely than previously thought and as the recent stock market instability has accelerated, so has the volume of targeted cyber attacks and their relative impact on the economy. In addition, security analysts believe the recent spike in malware could be related to cyber-criminals now having fewer possible targets as a result of consolidation within the banking industry [2][18].

2. Methodology study

This study is based on a descriptive study. Researchers have adopted a lot of sources that deal with cyber crime in all its forms, to study and draw conclusions in the midst of the global financial crisis to identify the factors that contributed into increasing cyber attacks and make appropriate recommendations.

3. Cybercrime

Cybercrime refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. cybercrimes are more properly restricted to describing criminal activity in which the computer or network is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. As the use of computers has grown, computer crime has become more important [3].

4. Spam

Unsolicited sending of bulk email for commercial purposes. E-mail spam, also known as junk e-mail, is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail.. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk..

E-mail spam has steadily, even exponentially grown since the early 1990s to several billion messages a day. Spam has frustrated, confused, and annoyed e-mail users [3][4].

5. Spammers and financial crisis

The worldwide financial crisis sparked an increase in spam production following the initial mid September collapse of Lehman Brothers Bank, Bank of America and AIG [4]. As the world's stock markets crashed,

spammers attempted to lure recipients by promoting services that claimed to eliminate or leverage debts, mortgages, and other fiscal or loan obligations.
A large spam wave targeting U.S. residents advertised the services of a company that allegedly offered to help stop home foreclosures.

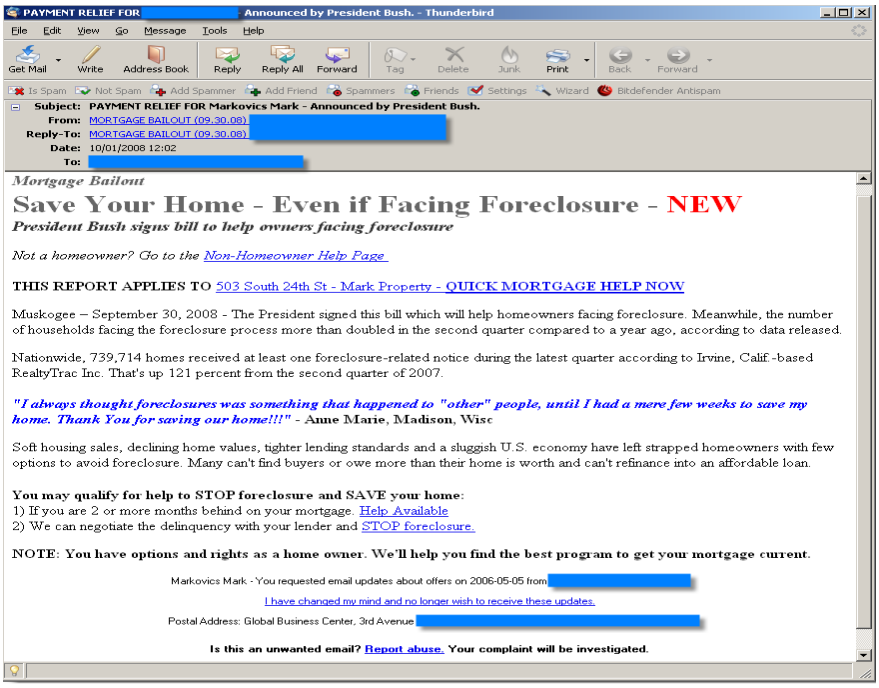

Figure 1 Example of spam that offered to help stop home foreclosures

Based on a template used before the recession, additional spam campaigns featuring financial ads gained significant volume. Usually limited to a single body or subject line, the messages direct users through Web links to various Web sites, most of which are involved in phishing schemes [5].

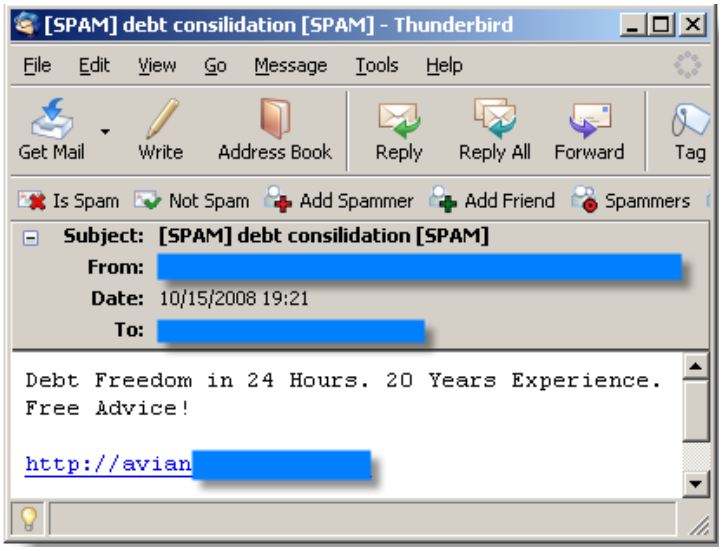

Figure 2 Example of spam that direct users through Web sites are involved in phishing schemes

Other spam waves used the economic crisis as a simple decoy for advertising drugs, pirated software or replicas. Finally, one of the most recent spam attempts relied on a multiple combination of automatically generated and distributed junk e-mails and social networking profiles directing the targeted recipients to Web sites where they can "leave debt behind."

Figure 3 example of spam used "leave debt behind" messages

Spammers have been using the current economic state and computer users' worries to their advantage by targeting spam campaigns towards those looking for not only more information about the recession but also those looking for how to better their current financial status

6. Financial crisis and cyber-crime surge

When we began looking into the specific effects cyber-criminals had on the economy during times of duress we found a startling connection: the criminal economy is closely interrelated with the global economy. Based on extensive research and analysis of emerging malware patterns, we believe that criminal organizations are closely watching market performance and adapting as needed to ensure maximum profit [5][6].

The new strategy appears to be developed in response to banking industry consolidation brought on by the multi-million-dollar bank bailout packages introduced by several governments around the world. As a result of this consolidation, fewer banking entities will exist in the long term and the perception of instability in the financial community makes for a less attractive target. This situation has increased the volume of other types of malware such as adware, which under normal circumstances would be second to Trojans [3][4].

Cyber-criminals have to increase their activity to reach more users with campaigns designed to put money directly into their pockets, especially during times of economic instability. For example, there is a surge in the number of fake antivirus software scams that trick unsuspecting consumers into making an online transaction, instead of criminals relying heavily on phishing the credentials for banks. Data shows that these fake antivirus campaigns are generating over €10 million in profits each month for the underground economy [2][6].

All of this is achieved simply by creating thousands of variants of a new type of adware and distributing it across the Internet. Users can be infected in several ways: browsing Web pages with adult content; downloading files from peer-to-peer networks; responding to e-greetings; downloading files that exploit security holes so users are infected without realizing.

These infected programs all operate in a broadly similar way: The program tells users that they are infected and pop-up windows, desktops and screensavers keep appearing, preventing the victim from using the computer. The aim is to scare the user into buying the fake antivirus with, for example, cockroaches 'eating' the desktop, or fake blue screens of death [2][8].

During the purchase process, users are asked to enter confidential data. On average, their credit cards are charged €49.95 for an 'antivirus' that they never receive. "As the products are imitations of well-known brands, the victims often turn to the companies, who can't do anything as they have not really bought any licenses" [9][21].

What still unknown is whether the bank or credit card details are then used later by the cyber-crooks. If that were the case, the financial implications are even greater.

Now however, cyber-crooks operate in organized mafias with purely financial motives. They bombard the user community with thousands of new variants of each of the malware families every day. In doing this they hope to saturate antivirus laboratories and at the same time avoid the kind of media attention given to single-virus epidemics. Users therefore have a false sense of security.

As US stock market declined the activity on the "malware markets" was the opposite: it grew substantially.

As Dow Jones Industrial Average, NASDAQ, S&P 500 and Composite Index all dropped from the plus 0.0 percent range to approximately negative 6.0 percent or lower. In the same period the Spanish IBEX 35 index and the London FTSE 100 also suffered major losses. The same timeframe witnessed a significant surge in daily malware threats from 10,150 to well over 24,000 [10][2][20].

As stock markets dropped from -0.5 to -5.5 percent while daily threats grew 50 percent each day, from 8,276 to over 31,404 at the same timeframe.

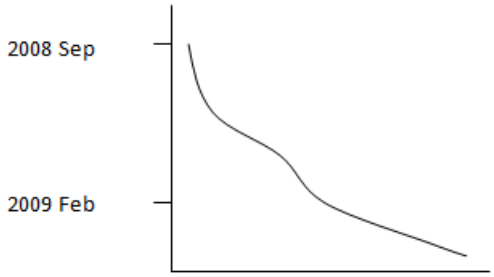

Figure 4 Stock markets trend

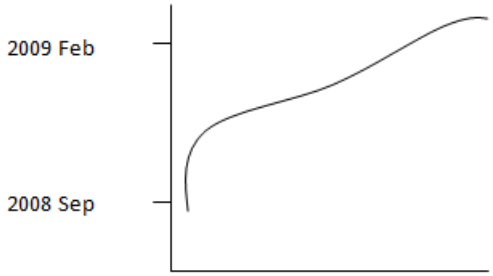

Figure 5 Malware threats trend

7. Spam, Scam, phishing Statistics

Statistics regarding internet scams and frauds are presented here as a snapshot in time 2008-2009. Web crime statistics are notoriously difficult to obtain, with many sources each calculating them in a different manner and different time frame, using a different source, we use the Internet Crime Complaint Center's (IC3) and MessageLabs Intelligence statistics as a baseline.

It is clear that the trend of mail and spam took an upward-trend and still moving in this direction, because the ability to take benefit of the financial crises is still possible. The greater the scope of the problem means increasing in the appetite of the cybercrime. Figure 4 shows the upward-trend of spam and mail [11].

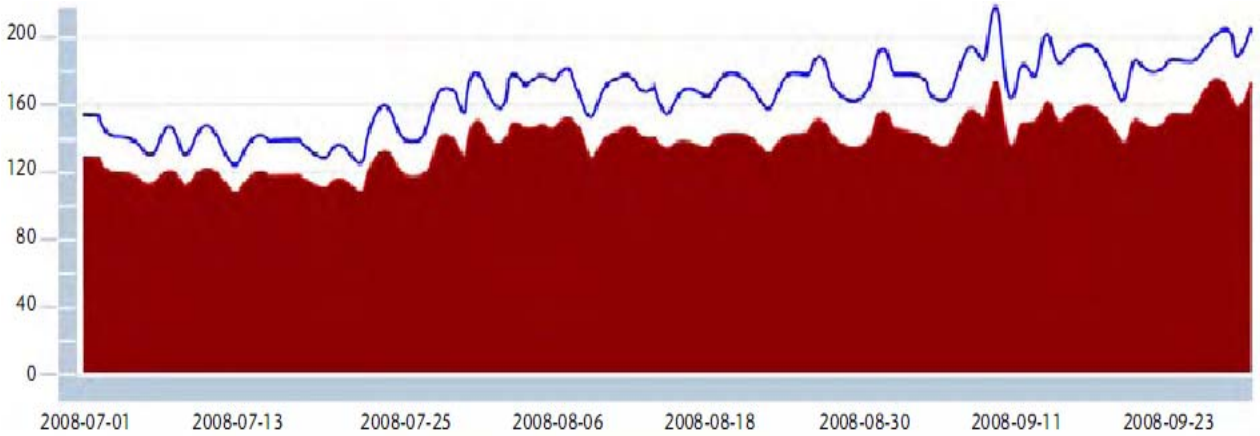

Figure 6 General Mail and Spam Trends [11]

It is clear that viruses and spam rates increasing rapidly from December 2008 till now, because the global financial crisis continued to feed the appetite of the spammers. Figure 7 shows e-mail connections, spam, viruses and phishing trend from October 2008 to February 2009 [12].

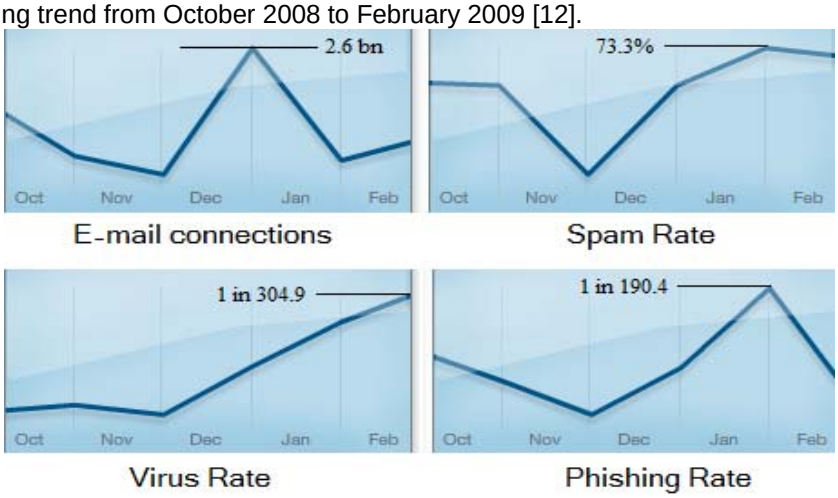

Figure 7 E-mail connections, spam, viruses and phishing trend [12]

Because the roots of the world financial crises began in the United States of America; percentage of Spam originating in U.S. Doubles, with Election-related Spam Messages Topping 100 Million Daily. Taking advantage of great panic, lack of information, uncertainty and the hope to save what can be saved [12][11]. Table 1 shows statics of Geo-Location of Spam by Country

Table 1 Geo-Location of Spam by Country

Country	***Spam percentage***	***Country***	***Spam percentage***
United States	32.1%	Great Britain	3.3%
Turkey	6.3%	China	3.2%
Russia	5.2%	Columbia	2.9%
Brazil	5.0%	Argentina	2.3%
South Korea	3.9%	Thailand	2.1%
India	3.5%	Spain	2.09%
Other	28.2%		

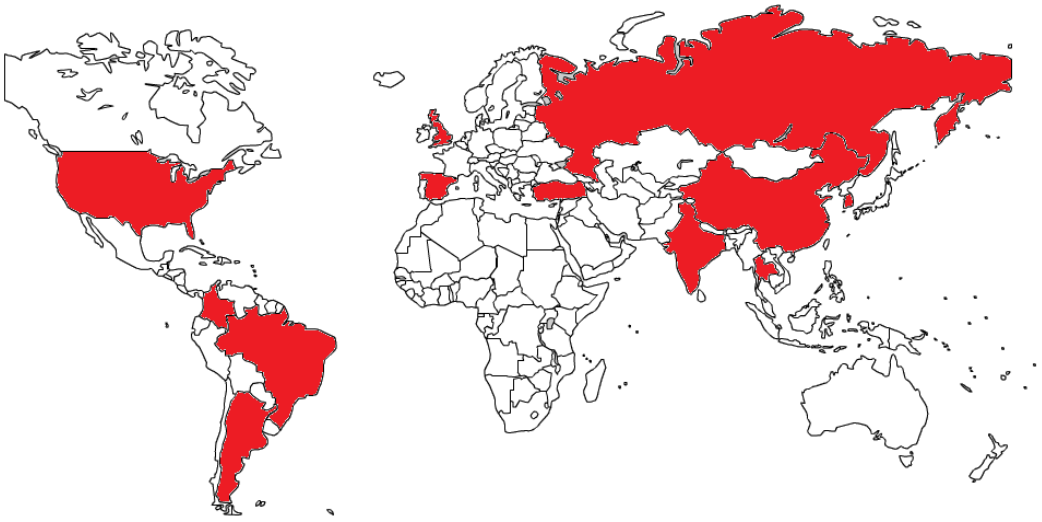

Figure 8 Map of Geo-Location of Spam by Country [11]

8. Spam Messages

Image spam declined to less than 2% of spam during 2008 from its peak at 20% in summer 2007. The majority of spam is now made up of text-only or HTML spam. Spam messages have also become shorter and terser containing only one or two sentences and usually a link to a Web site. This makes it much harder to identify the true nature of the spam message using anti-spam techniques employing contextual analysis of the words in the message.

During the latter half of 2008, and prior to the disruption in November of the botnets responsible for much of the spam in circulation, spam messages had become shorter in length and predominantly using plain text or HTML content. With greater capacity available to the botnets, many of the individual spam runs had also increased in volume [13].

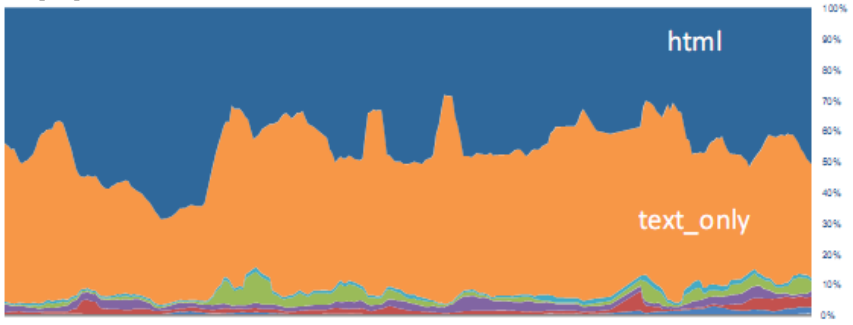

Figure 9 Spam messages format [13]

9. Recession spam

New spam approach appeared that could be described as *"recession spam."* It contained text such as :

"Money is tight, times are hard. Christmas is over. Time to get a new watch!"
"Affordable brand name watches"
"Get 15% off these"
"Cheaper than you could imagine"

The same messages also include links to a major well-known search engine, it is not actually using an automated re-direction link, nor is it actually searching for keywords hoping that the spammer's site appears first in the results. Instead, it is simply searching for the spammer's domain, in the seemingly hopeful probability that this particular search engine has not indexed the target site.

Search engine spamming is a technique that allows the spammer to include a link constructed from a search engine query within the email. When the link is followed, the browser is led to the spammer's website. This means that the spammers can send messages without directly using the URL for the spam site in the body of the message, which makes it more difficult for traditional anti-spam products to identify the message as spam. While spam filters may recognize known spam sites, they cannot reasonably block links to legitimate search engine sites without imposing significant collateral damage [13][14].

10. Conclusions

The strength of the internet in terms of its ease of accessing and sharing content electronically has become one of its weaknesses. A key observation that can be drawn is that the internet has influenced the world of organized crime and the criminal marketplace. The internet has resulted in new avenues for traditional crime and has also opened up a whole new area of criminal activities.

Because of uncertainty, panic and the greater sense of money to be made a lot of the financial loss due to organized cybercrime has been increased by increasing the use of bonnets which led to lost tens of millions of dollars from "pump and dump" schemes in which criminals buy and sell stocks with other people's account information harvested online [15][16].

Financial institutions face a very serious challenge and it's likely to grow more serious as time passes [6], which means the need for a network response to deal with a network attack based on advanced warning system to prevent such cyber attacks [17]

11. Recommendations

1. Government must use new and advanced strategies for detecting fraud to combat financial crimes.
2. Computer users have to learn how to deal with rogue traders, fraudsters, embezzlers and computer criminals.
3. Obtain hands-on advice on how to conduct fraud investigations from a practitioner's point of view.
4. Prevent internal fraud within organizations by developing an effective fraud risk management framework.
5. Promote anti-money laundering awareness and foster a culture of compliance and honesty by understanding the importance of corporate governance.
6. Identify key opportunities in fraud detection by examining advanced anti-money laundering and terrorist financing detection strategies.
7. Implement effective measures and customer due diligence to prevent money laundering activity.
8. Move to enact legislation to enable law enforcement to investigate crime in the face of rapidly evolving communications technology and prevent criminals from taking advantage of new technologies to hide their illegal activities from the law.
9. Designate an existing government agency to manage the Cybercrime file.
10. Update the criminal code, reflective of the modern techniques and technologies employed in cyber crime, with deterrents which are substantial and effective.

References

1. Robert j. Shiller with George Akerlof, Animal Spirits (2009), How Human Psychology Drives the Economy And Why It Matters for Global Capitalism Princeton University Press.
2. PandaLabs Uncovers Direct Correlation between US Stock Market Declines, Banking Industry Consolidation and Surges in Economic Cyber-crime (10/23/2008). "Recent Stock Market Decline Causes Economic Cyber-Crime to Hit All Time High, According to PandaLabs". http://www.pandasecurity.com/homeusers/media/pressreleases/viewnews?noticia=9405. Retrieved on 2/23/2009
3. Computer crime. From Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Cybercrime. Retrieved on 3/23/2009
4. Help net security. "Increase in spam productivity due to world financial crisis" (31/11/2008). http://www.net-security.org/secworld.php?id=6703. Retrieved on 3/24/2009.

5. BitDefender press center, “BitDefender Researchers Find Increase in Spam Productivity Due to World Financial Crisis” (3/11/2008). http://www.bitdefender.com/NW869-en--BitDefender-Researchers-Find-Increase-in-Spam-Productivity-Due-to-World-Financial-Crisis.html. Retrieved on 3/26/2009.
6. Ryan Sherstobitoff, Pandalab plog. “As stock market drops malware rises” (21/11/2008). http://pandalabs.pandasecurity.com/archive/As-stock-market-drops-malware-rises.aspx. Retrieved on 3/26/2009.
7. B. Mark Smith, A History of the Global Stock Market: From Ancient Rome to Silicon Valley, ISBN-13: 9780226764047, University of Chicago Press, 2004
8. PandaLabs. “30 million computers are infected by fake antivirus programs generating profits for cyber-crooks of more than €10 million every month” (15/10/2008). http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9394. Retrieved on 3/26/2009.
9. IT news Africa, 3”0 million computers infected by fake antivirus programmes” (24/11/2008). http://www.itnewsafrica.com/?p=1556. Retrieved on 3/27/2009.
10. PandaLabs, “Recent Stock Market Decline Causes Economic Cyber-Crime to Hit All Time High, According to PandaLabs” (23/10/2008). http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9405. Retrieved on 3/26/2009.
11. Consumer Fraud Reporting Crime Statistics, Internet Fraud, Scam and Crime Statistics – 2008. http://www.consumerfraudreporting.org/internet_scam_statistics.htm. Retrieved on 3/26/2009.
12. Marshal 8e6, TRACElabs. “Spam Statistics” http://www.marshal8e6.com/TRACE/spam_statistics.asp. Retrieved on 3/26/2009.
13. MessageLabs Intelligence. “Spammers Exploit New Year Diffidence – Financial Uncertainties and Personal Insecurities” (30/1/2008). http://www.messagelabs.com/resources/press/9881. Retrieved on 3/26/2009.
14. Keith Ferrell. MessageLabs, “Recession Spam Volume Shows No Recession In Spam” (25/2/2009). http://www.bmighty.com/blog/main/archives/2009/02/recession_spam.html. Retrieved on 3/26/2009.
15. Cnet News, “Week in review: Market whiplash” (17/11/2008). http://news.cnet.com/8301-1001_3-10068620-92.html. Retrieved on 3/26/2009.
16. ZDNet.co.uk “Security threats Toolkit: FBI warns of rising cybercrime threat” (16/10/2008). http://news.zdnet.co.uk/security/0,1000000189,39518856,00.htm. Retrieved on 3/26/2009.
17. Elinor Mills, Cnet News,” Homeland Security secretary proposes 'Manhattan Project'” (4/8/2008). http://news.cnet.com/8301-10784_3-9914391-7.html. Retrieved on 3/27/2009.
18. John Y. Campbell (2008), Asset Prices and Monetary Policy, ISBN-13: 9780226092119, University of Chicago Press,
19. Sebastian Edwards, Márcio G. P. Garcia, Financial Markets Volatility and Performance in Emerging Markets (2008), ISBN-13: 9780226184951, University of Chicago Press.
20. Steve Fraser, Wall Street: America's Dream Palace (2008), ISBN-13: 9780300117554, Yale University Press.
21. Ranald C. Michie, The Global Securities Market: A History, ISBN-13: 9780199280612, ISBN-13: 9780199280629 , Oxford University Press, 2008