How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession

By Peter Guerra

BlackHat 2009 Turbo Talk Whitepaper

Abstract

It is widely accepted that malware and botnets are established predominately to conduct cyber crime. The purpose of this paper is to paint a broad overview of the link between information security and economics and to discuss some research on the link of the CAN-SPAM Act of 2003 and the exponential rise of malware, botnets, and cyber crime. Using economic theory, I hope to spark an interest in economics as a discipline and to show how perverse economic incentives can give rise to unintended information security consequences.

Economics and Information Security

The ties between the disciplines of economics and information security were initially explored in the seminal work by Ross Anderson (Anderson, 2000). The Workshop on the Economics of Information Security (WEIS) is the preeminent place where these topics are typically researched and discussed. It is generally accepted that economics can help to explain why the state of information security is so dismal.

However, it is worthwhile to first describe the following basic economic principles that apply to information security (Frank and Bernanke, 2007):

- The Scarcity Principle – Having more of one good thing usually means having less of another. Also known as security trade-offs.
- The Cost-Benefit Principle – Take no action unless its marginal benefit is at least as great as its marginal cost. Often associated with attack profiles.
- The Incentive Principle – Cost-benefit comparisons are relevant not only for identifying the decisions that rational people should make but also for predicting the actual decisions they do make.

All three of these principles help to explain different failures associated with information security. Cost-benefit and scarcity help to explain why information security typically does not get the same share of resources as other IT groups. The incentive principle helps to explain why information security is often missing from large products, such as early iterations of Microsoft Windows (Anderson, 2009).

Another economic theory that is used frequently in literature is the Tragedy of the Commons, which describes how a common resource is used up by multiple individuals acting independently in their own self-interest (Hardin, 1968). Many researchers have made the analogy that the Internet is the commons, and no one self-interested individual or group is incentivized to protect the whole. For example,

while individual users may be incentivized to purchase anti-virus to protect their system, they would probably not purchase software to stop attacks against a third party, such as Amazon.

The Lemon Market economic theory also predicts that information technology products will be inherently insecure (Anderson, 2009). Security in products is a trust good. Because a buyer is unable to distinguish between a good used car and a lemon, they are only willing to pay the amount for a lemon, so the price drops. In general, secure products are indistinguishable from insecure ones, so companies are less incentivized to produce secure products because the buyer is unable to tell the difference.

So in essence, economic theory can explain the perverse incentives that create the current state of security.

Worldwide Economic Crisis

The current worldwide economic crisis has caused recessions in more than 100 countries around the globe. Many factors have contributed to this recession, but one key aspect, the globalization of capitalism, has made the impact more global than with previous recessions. Globalization refers to the global free trade of specialized goods and services between nations. For example, the US exports steel to Japan, and Japan exports electronics to the US.

With a global recession, emerging markets that have relied on the US for economic stability have felt the effect of the recession more deeply than others. The so-called emerging market, or BRIC countries (Brazil, Russia, India, and China), are currently experiencing recessions that are severely affecting their economies (Roubini, 2009). These countries have also historically invested large amounts of money to produce technologically skilled workers.

Brazil has invested many millions of dollars to get its country's Internet infrastructure completed. India's technology revolution is the direct result of the massive outsourcing of IT and software development to the country. The Chinese government has invested heavily in education and technological infrastructure. And finally Russia, after the collapse of the Communist government, now has a large organized criminal element that has been actively recruited former computer specialists to conduct cyber crime campaigns (Krebs, 2007).

Cyber Crime

Cyber crime is often defined as a crime committed online with the aid of a computer or networks. Typical activities of cyber crime can include the following:

- Child pornography
- Botnets
- SPAM
- Identity theft

- Fake security software
- Credit card fraud
- DDoS Extortion
- Click fraud
- Cyber squatting
- Blackhat SEO
- Pump-and-dump stock schemes

Of these, botnet creation has grown exponentially over the last 4 years. Botnets are created to be rented out for their combined computing power to send SPAM, host phishing sites, or sell fake anti-virus software. Some estimate that botnets now compose almost 27% of malicious activity on the Internet (Rajab, 2006). To calculate how much bot herders make creating and maintaining their bots, let's look at the economics of a SPAM campaign in the following table (Zink, 2008):

Spam Sent	40 million
Click-through ratio	0.12%
Total click-throughs	48,000
Click-through--sales ratio	1/200
Total sales	240
Total sales revenue	$37,440.00
Spammer commission rate	50%
Total SPAMmer income	$18,720.00
Weekly Costs	
Bulletproof hosting	$230.00
4 days of botnet access	**$6,800.00**
Email addresses	$4,000.00
Total Costs	$11,030
Net Weekly Profit	$7,690.00

Using these figures, is estimated that the yearly profit for one SPAMmer is around $340,000. This is a huge amount of money for a minimal amount of work. So a little extrapolation – if a SPAMmer does this on a weekly basis, he is using a botnet weekly. So we can calculate that $6800/4 = $1700 per day * 365 = $620,500 possible yearly net for a botnet herder. This is just for the rental of one botnet, which can be maintained by a small group of cyber criminals. This amount of return on a little investment of capital and with few repercussions makes this an extremely attractive option for cyber criminals.

In addition, Malware-As-A-Service and other market efficiencies are starting to crop up in the criminal underground, pointing to a sophisticated business model in which people are specializing in a way that is seen in mature markets (Danchev, 2008).

CAN-SPAM and the rise of Botnets

The CAN-SPAM Act of 2003 outlined ways that the US Federal Government, specifically the Federal Trade Commission, can go after spammers and apply criminal and civil penalties for violating the Act. The law is designed to also give Federal Law Enforcement the ability to take offline data centers that are responsible for the deluge of SPAM (Goodchild, 2008).

There have been two recent cases of the FTC shutting down ISPs that were accused of spamming: McColo and 3TSP. The removal of these ISPs actually had an impact on global SPAM rates, but only in the order of 20% (Clayburn, 2008). The majority of SPAM is sent through botnets, which are established through advanced malware campaigns. Now, SPAM has returned to the same level as before the McColo takedown.

The growth of botnets post-CAN-SPAM legislation has some wondering whether the threat of closing previously legal hosting businesses that sent SPAM drove the market to the cyber crime underworld. The supply and demand of SPAM remains high, even to this day. The increase in SPAM, malware, and botnets is correlated with a timeline consistent with the CAN-SPAM campaigns.

I believe that it can be posited that the rise of modern advanced malware is a direct result of SPAM campaigns over botnets. Because the fear of losing money by being shut down by the FTC after the passage of CAN-SPAM, most spammers started to send SPAM through rented channels such as botnets. This, in turn, has fueled an increase in advanced malware tactics to bypass traditional security mechanisms. This is an example of capital markets doing what they do best: increasing specialization for increased efficiency and cost.

For this to be true, the argument that botnets have grown substantially over the last 4 years must be explored. Because malware and botnets are often linked, one way to measure the growth of botnets is to look at the number of malware signatures that anti-virus vendors distribute. In Symantec's 2009 Threat Report, it indicated an increase in 2008 of more than 165% of the number of unique pieces of malware that it detected in 2007 (Symantec, 2009).

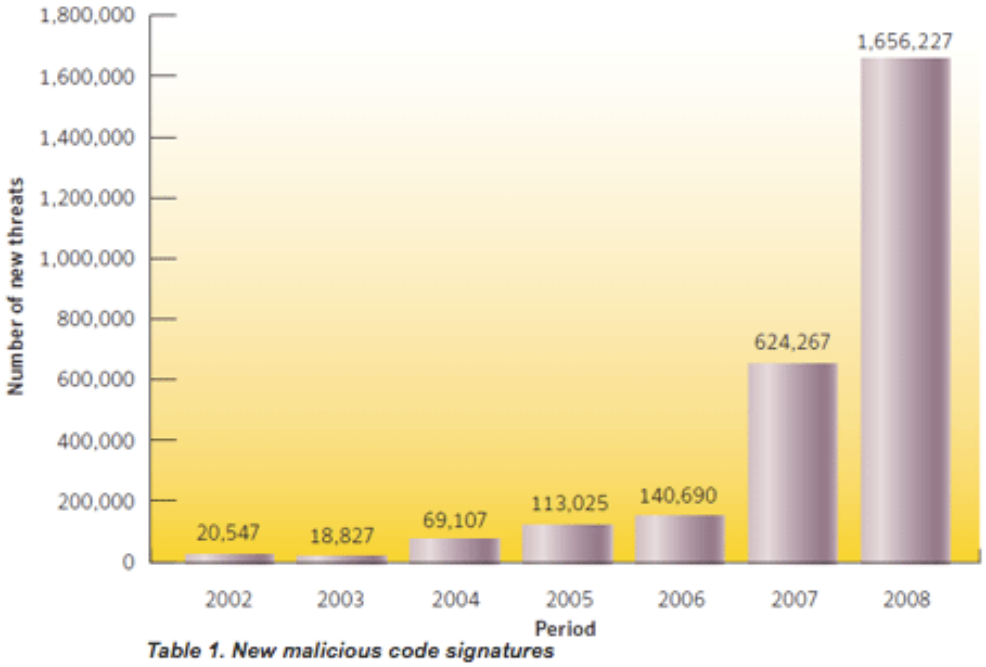

Table 1. New malicious code signatures

Source: Symantec Corporation

Keeping in mind that CAN-SPAM Act was passed in 2003, the chart above shows a significant year-over-year increase in the number of unique malware signatures. It is growing exponentially from 2003 through 2008.

Tying it Together

We have perverse economic incentives that point to weak information security. We have a global recession that will put skilled IT workers out of work. We are globally connected in every way possible through modern networking. And we have a weak global regulatory and legal framework to prosecute cyber criminals. In addition, the recession is pulling our attention and our resources away from information security needs.

During a recessionary period in the US and other countries, one would expect that certain types of petty crimes such as robbery and muggings would increase in years of economic downturns. We asked the question: Will cyber crime increase in a time of global economic recession? One study by KMPG found that many enterprises believed that the recession put their business at greater risk from out-of-work IT workers tempted to join the criminal underground to make ends meet (Kirk, 2009).

I believe that the data are pointing to a perfect cyber storm that is heading our way. We have been vulnerable, and we will be worse off because of the recession and globalization.

It is acknowledged that there are probably many different factors that have resulted in the increase of cyber crime and associated malware, besides just CAN-SPAM.

Internet users are increasing year over year, and many of these are relatively unsophisticated, the type that are ripe for exploitation.

Also, in recent years, the barrier to entry for exploiting machines and creating botnets has decreased dramatically. Whereas it previously took experts days or weeks to exploit an unknown vulnerability, cyber criminals can now purchase an advanced malware capability for as little as $300 on the open market (Danchev, 2008). This could also fuel demand for botnets and malware.

Conclusion

Economic theory predicts that the global recession will probably increase the amount of cyber crime as the recession deepens. This could result from a variety of causes: an increase in attacks on more vulnerable and desperate people from those with cyber skills joining the cyber criminal ranks for needed income; and a decreased focus on and investment in computer security as a result of fewer resources.

It is acknowledged that given that the wealth of US households has shrunk by almost $1.4 trillion, so the total amount of money available to steal has decreased. It is also acknowledged that correlation and causation are extremely difficult to prove conclusively. One could argue that cyber crime has been increasing anyway because of the low barrier of entry, promise of e-gold riches, and virtually no risk of being caught and prosecuted. This is regardless of the state of the worldwide economy.

However, looking at the sophistication of workforce of the emerging markets, one can reasonably conclude that because the economic fortunes of these countries has been greatly reduced with less hope of improvement of their situation, cyber crime opportunities and workers will probably increase.

I believe that further research into the links between cyber crime, economics, and the recession is warranted and should be explored further. I also believe that a good understanding of the profit motives behind most modern cyber attacks will provide security practitioners with a more well-rounded perspective on the threats they are struggling against daily.

The important takeaway is for policy makers and information security professionals to acknowledge that often the policies and technologies are not effective in defending IT assets, and there are other invisible hands at play. By studying the link between economics and information security, we can obtain a clearer picture of the motivation for and prevention of cyber crime.

Bibliography

Anderson, Ross. *The Economics of Information Security*. 2000. http://www.cl.cam.ac.uk/~rja14/Papers/econ_science.pdf.

Anderson, Ross. *Information Security – Where Computer Science, Economics and Psychology Meet*. April 2009, De Montfort.

Claburn, Thomas. Spam Volume Drops When ISPs Terminate McColo -- Spam ISP Security -- InformationWeek. http://www.informationweek.com/news/security/client/showArticle.jhtml?articleID=212002194.

Danchev, Dancho. New Web Malware Exploitation Kit in the Wild. http://ddanchev.blogspot.com/2008/11/new-web-malware-exploitation-kit-in.html.

Frank, Robert, and Bernanke, Ben. 2007. *Principles of Economics*, *Third Edition*. McGraw-Hill Irwin.

Goodchild, Joan. Symantec Threat Report: Three Ways Internet Crime Has Changed - CSO Online - Security and Risk. http://www.csoonline.com/article/458170/Symantec_Threat_Report_Three_Ways_Internet_Crime_Has_Changed.

Goodchild, Joan. Why Cybercrime is Thriving - CSO Online - Security and Risk. http://www.csoonline.com/article/465919/Why_Cybercrime_is_Thriving.

Hardin, Garrett. "The Tragedy of the Commons", Science, Vol. 162, No. 3859 (December 13, 1968), pp. 1243-1248.

Kirk, Jeremy. *In poor economy, more IT pros could turn to e-crime*. InfoWorld News. http://www.infoworld.com/article/09/03/24/In_poor_economy_more_IT_pros_turning_to_ecrime_1.html.

Krebs, Brian. Shadowy Russian Firm Seen as Conduit for Cybercrime. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html.

Rajab, M., Zarfoss, J., "A multifaceted approach to understanding the botnet phenomenon," in 6th ACM SIGCOMM conference on Internet Measurement, SESSION: Security and Privacy, 2006, pp. 41–52.

Roubini, Nouriel. A Global Breakdown Of The Recession In 2009. Forbes.com. http://www.forbes.com/2009/01/14/global-recession-2009-oped-cx_nr_0115roubini.html.

Symantec Internet Security Threat Report trends for 2008. Volume XiV, published April 2009.

Zink, Terry. *Terry Zink's Anti-SPAM Blog : How much do spammers actually make?* http://blogs.msdn.com/tzink/archive/2008/08/28/how-much-do-spammers-actually-make.aspx. 2008.