

Running head: CRIME AND CYBERCRIME - IT'S ABOUT MONEY

Crime and CyberCrime - It's About the Money

William R. Wilson

Harvest Internet Solutions

Abstract

As the world economy with its banking, investing, commerce, and personal finance is moving rapidly onto the internet, the current and very ominous trend in cyber crime is that it is becoming predominantly financial in focus and an arena for increasingly-organized, professional criminals. Certainly there are other motives from cyber terrorism to the mischief of "script kiddies" (amateur vandals) but in the main, cyber crime is becoming all about the money.

As the world economy with its banking, investing, commerce, and personal finance is moving rapidly onto the Internet, the current and very ominous trend in cyber crime is that it is becoming predominantly financial in focus and an arena for increasingly-organized, professional criminals. Certainly there are other motives from cyber terrorism to the mischief of "script kiddies" (amateur cyber vandals) but in the main, cyber crime is becoming all about the money.



In 2000, at 16 years of age, Jonathan James became the first juvenile to be sent to prison for cybercrime including stealing software valued at \$1.7 million from NASA computers as well as hacking the U.S. Defense Threat Reduction Agency sever. By preying on the dominant network technology of his day, the Internet, he became a folk hero. Jonathan was a loner whose motive by his own admission was "I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off." (Ten Most Famous Hackers of, 2007)

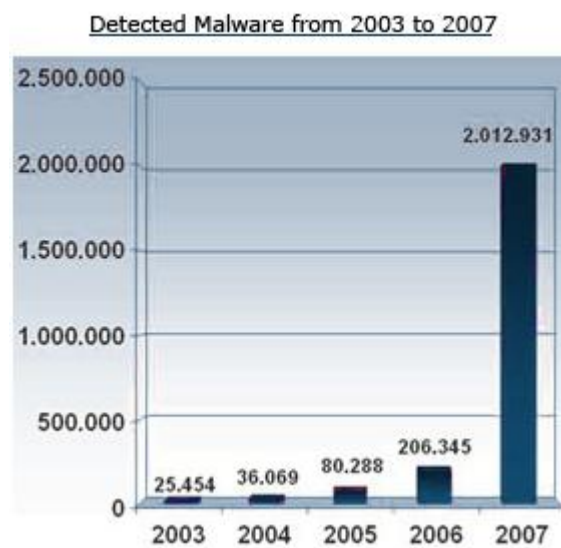


In 1863, at 16 years of age, Jesse James starts his life of crime in the American Wild West and goes on to commit multiple bank and train robberies with his gang over the next twenty years. By preying on the dominant network technology of his day, the railroads, he also became a folk hero. Not a loner like Jonathan, Jesse commanded a gang whose motivation was initially political after the defeat of the Confederate cause in the American Civil War but whose motivation eventually became simply a criminal campaign of widespread robbery. He attacked trains because that is where large amounts of money were distributed and vulnerable. (Patcher, 2005)

Similar to, but far eclipsing the railways of the late 1800s, large, very, very large amounts of money are distributed and vulnerable to the skillful criminal on the Internet.

Passing are the days when the primary motive of hackers faced with a challenging hack was that of British mountaineer George Leigh Mallory who when asked why he wanted to climb Mount Everest, replied, 'Because it's there'. (Knowles, 2001) As Jesse James criminal motive evolved from political rage into a purely financial one, so the primary motive of cyber criminals is also moving to financial gain. Even more disturbing is that the lone hacker is giving way, as in Jesse James' day, to organized gangs of cyber criminals, cybergangs.

The criminals of the American Wild West used dynamite, Colt revolvers and Winchester rifles as their tools and the vast unmapped spaces of the open country for their anonymity. Cyber criminals use malware and large herds of net bots for their tools that hide on PCs and servers across the great expanse of the Internet for their anonymity. Today's cyber criminal, unlike the hacker of the 1980s and 1990s prefers secrecy to celebrity that he might steal the more. There has been an explosion in this type of financially focused malware starting in 2007 as illustrated in the following chart and associated analysis.



“The statistics are alarming and clearly demonstrate that not only is there a lot more malware around than before, but also that the motivation of malware authors has changed. Now, their motivation is purely financial and there is an entire industry behind them, financing and encouraging them, and this means that they are becoming more professional.” (Panda Security, 2008)

Professional cybergangs are using the best technical skills money can buy to “virtualize” their real world activities because as the money was on the railroad network in 1880, it’s now on the Internet. Further, because of the international reach and openness of the Internet, cybergangs organize, plan and implement world-wide campaigns of crime from countries without “a legal framework to combat cyber crime.” (United Nations ESCAP (Economic and Social Commission for Asia and the Pacific), 2008) Although this criminal activity is kept quiet by the corporate targets for obvious reason of potential loss of consumer confidence, the extent of the threat is recognized by the Senior IT Manager for Lloyd’s when he writes in 2008 that:

“Cyber crime is more often than not perpetrated by organized criminals with the intent of financial gain. It is covert in nature; the longer it remains undetected, the greater the financial gain. Organized crime is now reaping such significant rewards that criminal gangs are investing more in their work which leads to a vicious circle because it generates an increase in frequency and sophistication of attacks.” (Alldrick, 2008)

The commandment “Thou shall not steal.” a basic tenet of man’s conscience and the legal codes of diverse cultures, has been necessary and, sadly, widely ignored for at least 3500 years. Whenever men have used their ingenuity and enterprise to earn and protect wealth, others have used theirs to take it. On July 21 1873 the James gang carried

out their first of many train robberies by derailing and then robbing the Rock Island, Iowa Train. (Patcher, 2005) With the same ruthlessness and motive, one hundred and thirty five years later, a Russian cybergang cleans out the retirement accounts of hundreds of workers in the United States. Whether in the industrial age or the information age the evidence remains clear and common wisdom will heed it: The technology changes, the nature of man remains unchanged.

References

- Alldrick, M. (June 24, 2008). Lloyd's Senior IT Manager Marcus Alldrick on cyber crime... Retrieved October 31, 2008, from LLOYD's of London Corporate Website:
http://www.lloyds.com/News_Centre/Features_from_Lloyds/Lloyds_Senior_IT_Manager_Marcus_Alldrick_on_cyber_crime_240608.htm
- Knowles, E. (2001). A Quote from George Leigh Mallory. Retrieved November 3, 2008, from AskOxford.com:
<http://www.askoxford.com/worldofwords/quotations/quotefrom/mallory/>
- Panda Security. (2008). Cybercrime. Retrieved October 31, 2008, from
<http://www.pandasecurity.com/homeusers/security-info/cybercrime/>
- Patcher, A. (2005, December 5). American Experience - Jesse James. Retrieved November 3, 2008, from Public Broadcasting System Website:
<http://www.pbs.org/wgbh/amex/james/>
- Ten Most Famous Hackers of All Time. (2007). *ITSecurity*. Retrieved November 3, 2008, from <http://www.itsecurity.com/features/top-10-famous-hackers-042407/>
- United Nations ESCAP (Economic and Social Commission for Asia and the Pacific). (2008). Information Security for Economic and Social Development. In. Retrieved October 31, 2008, from
<http://www.unescap.org/icstd/policy/publications/Information-Security-for-Economic-and-Social-Development/>