Examination of Cyber-criminal Behaviour

H. Jahankhani, Ph.D.
University of London, UK
Email: hamid.jahankhani@uel.ac.uk

Ameer Al-Nemrat
University of London, UK
School of Computing, IT and Engineering

Abstract

Cybercrime is the world's biggest growth industry and is now costing an estimated €180 billion loss to organisations and individuals, every year. The creation of 'virtual identities' gives a greater anonymity to the activities of organised criminals. Today our commonwealth is protected by firewalls rather than firepower. This is an issue of global importance as new technology has provided a world of opportunity for criminals. As a consequence law enforcement agencies all over the world are struggling to cope. Therefore, today's top priority is to use computer technology to fight computer crime.

Keywords: Cybercrime.

Introduction

Since time immemorial criminal activity has by its very nature drawn together many potential perpetrators of crime. Historically this activity led to an underclass, which in the United Kingdom was countered in Sir Robert Peel's principles of early policing. The original London "peeler's" communicated by means of a whistle. Later the telephone provided the police of the day with a distributed network of communications posts. These are evidenced by the police boxes which were installed throughout the major cities in the United Kingdom during Edwardian times.

This network provided a means by which the embryonic command and control perspectives were developed for the early metropolitan police forces. In the United States this concept was replicated, most notably in the crime ridden cities of Chicago and Boston. During prohibition these two cities had witnessed the growth of organised crime against a background of criminal focussed families, some of which were of Italian extraction and for whom the "Mafia", label became a badge. Such criminal activities are however not the sole domain of any particular nation or ethnic group. For example the activity of East London gangs, Chinese "triads", eastern European and Asian criminal groups having been particularly significant within the UK during the last 50 years. The means to communicate provides both the law enforcer and the criminal with

the ability to direct resources and share information within their communities, in order to maximise their operational efficiency, flexibility and speed of response. While the means are identical the ends are clearly not. Indeed it is therefore no surprise that the criminal elements have used communications to further their aims since the 1920s.In particular with the development of early telephone systems into the new telecommunications systems, including the Internet and mobile technologies, have created opportunities for such criminal groups to disseminate information of value in a timely manner.

In many ways, cybercrime is no different to more traditional crime – both involve identifying targets, using surveillance and psychological profiling. The major difference is that the perpetrators of cyber-crime are increasingly remote to the scene of the crime. The traditional idea of a criminal gang loses its meaning as members can now reside on different continents without ever having to actually meet.

Cybercrime

E-security is an issue of global importance and the methods cyber-criminals use are far-reaching, cunning and technologically advanced. Criminals search out the services of thrill-seeking hackers and 'script kiddies' to provide the expertise they need, which can be seen as a modern form of child labour.

The concern about cybercrime prevention has increased significantly among politicians, security specialist, academic institutions and legal professionals, with a staggering array of methods in an attempt to reduce the level of cybercriminal activities in the society.

In the EU and USA, the decision to focus on implications of technical methods for fighting cybercriminal is not arbitrary but comes from the need to do so after the 9/11 attacks. According to Suleyman Anil, who is in charge of protecting NATO against computer attacks, "Cyber defence is now mentioned at the highest level along with missile defence and energy security. We have seen more of these attacks and we do not think this problem will disappear soon".

International money laundering is a particular concern in the arena of cybercrime as it can be used to finance and support criminal activities. Internet banking and digital cash are the most common ways of washing dirty money. Criminals try to hide and cover the sources from which their money comes by creating complex layers involving 'social engineering' - tricking innocent parties into divulging sensitive information. Phishing, Pharming, Spyware, Bin Raiding and Public Records Access are just some of the common techniques used by the criminals. Also, money launderers are moving to exploit other poorly defended message transmission systems and emerging technologies, such as Voice over Internet Protocols (VoIP).

Phishing is an effective means of gathering valuable personal and organisation information. Phishing is one end of a two-ended criminal enterprise in that it is the gathering of the information and the second part is the utilisation of that information for criminal purposes. Phishing is mainly conducted through the medium of email given the ease of use and the relative anonymity of email use. Criminals are able to 'mass email' potential victims masquerading as their bank or other party who might have a legitimate interest in contacting them about financial matters. The emails are crafted in such a way as to appear as though the request for the information e.g. names, dates of birth, mother's maiden name, account details etc. is being legitimately made. In reality it is not and many willingly provide this information only later to discover that they have unwittingly passed them to an identity thief. Once in possession of this information the thief can use it to steal an individual's or organisation's identity and divert money away from them.

Bin Raiding is a method of obtaining information applies equally to individuals and organisations. As the name suggests, a criminal can rout through dustbins to obtain valuable information about an organisation. This includes obtaining bank account and credit card details, computer passwords, letterheads, signatures and other information which either on their own or added to other information allow a criminal to gain access to an organisation's accounts or those of its clients, trading partners, or suppliers. In a survey commissioned by the security company, Fellowes, it was estimated that 97% of households, approximately 21 million homes, disposed of information that could be exploited by identity thieves by throwing it in their household refuse, (Leyden, 2006).

In the UK it has long been the case that certain personal and business records are freely accessible to the public through Public Records Access. Personal details may be obtained by the payment of a small fee to the General Register Office for documents such as certificates of birth, death, marriages and civil partnerships and there is no scrutiny of the identity of the applicant. Business details and records are obtained in a similar way from Companies House. These resources represent a rich source of information for identity thieves who are then able to utilise them for the purposes of duplicating an identity. Information from the latter source has been used in order to take over a company's identity entirely by altering the details to the thieves' advantage.

Cross-border cybercrime poses a real threat to global security. Many countries do not have laws in place to combat it, and the international legal framework is patchy. By creating complex and difficult-to-trace internet layers, which cut across many national borders or, by tricking individuals into releasing their personal data; organised crime is often able to operate virtually undetected.

Internet has all the ingredients needed by organised crime to pursue its damaging business: it's global, it's fast and it's virtual. In the wrong hands, this adds up to the

potential to make vast sums of money illegally. In the early days of computers, 'computer crime' meant breaking into, or stealing, a single PC. Today, the term spans a wide range of fast-evolving offences. Broadly speaking, cybercrime can be divided into two categories;

- New crimes that are a result of Internet and can only be committed online
- Old-style crimes that use hi-tech and going online

Organised criminals have the resources to acquire the services of the necessary people. The menace of organised crime and terrorist activity grows ever more sophisticated as the ability to enter, control and destroy our electronic and security systems grows at an equivalent rate. Today, certainly email and the Internet are the most commonly used forms of communication and information-sharing. Just over one Billion people use the internet every day. Criminal gangs 'buying' thrill-seeking hackers and 'script kiddies' to provide the expertise and tools, this is called cyber child labour.

Cybercrime Profiling

Researchers from different disciplines have attempted to explore different dimensions of the issues surrounded cybercrime behaviour. To date however, despite numerous attempts, there is a lack of agreement on frameworks for either understanding and/or responding to these issues, their impacts and their interrelationships (Broucek & Turner, 2006). The lack of classification system is significant handicap and may be due to the considerable confusion that occurs around the very notion of what constitutes "Cybercrime" or computer – related crime and indeed whether it is new or old crime in a new bottle (Broadhurst & Chantle., 2006).

In order to develop useful profiles of different offender categories, a large amount of data is required and in order to improve the reporting of cybercrime, there are needs to increase the trust between the public and private sectors, which will result in reporting of cybercrimes when they occur. This will allow researchers to more precisely identify whether or not any unique patterns and characteristics actually exist.

In order to understand the new trends of the cybercrime and also establishing the appropriate framework that will be the foundation stone to investigate and prosecute the cybercriminals, there is an urgent need for cooperation and harmonisation of public and private sectors to encourage cybercrime reporting. Understanding the steps in the process of committing crime, and understanding the conditions that facilitate its commission, helps us to see how we can intervene to frustrate crime"(Wilson, R. 2006).

Criminal profiling is the process of Investigating and examining criminal behaviour in order to help identify the type of person responsible (Turvey, 2002). The FBI's Hayelwood and Douglas 1980, sited in Johnson 2005, (Johnson, 2005), defined profiling as - *An educated attempt to provide...specific information as to the type of individual who committed a certain crime.... A profile based on characteristics patterns or factors of uniqueness that distinguishes certain individuals from the general population.*

To date, all the national security organisations depend on data and text mining techniques to detect and predict criminal activities, while data mining refers to the exploration and analysis of large quantities of data to discover meaningful patterns and rules, (Kanellis, Kiountouzis, Kolokotronis & Martakos, 2006). Text mining, sometimes refers to as text data mining, is the process of analysing naturally occurring text for the purposes of extracting and non trivial patterns or knowledge from unstructured text (Kanellis, Kiountouzis, Kolokotronis & Martakos, 2006). The objective of many intelligence data analysis projects is to use data mining to find association and/or discover relationships among suspect entities based in historical data, while data mining analysis data from structured database, there is a large volume textual data (e.g e-mail, telephone conversation and text messages), which crime investigators have to examine which are unstructured.

Data mining is a powerful tool that enables criminal investigator who may lack extensive training as data analysts to explore large database quickly and efficiently. The following are some of the very common techniques;

a) Entity extraction: the process of identifying names, places, dates, and other words and phrases that establish the meaning of a body of text—is critical to software systems that process large amounts of unstructured data coming from sources such as email, document files, and the Web. By locating certain types of phrases and associating them with a category, applications such as text analysis software can perform functions such as concept extraction.

b) Clustering technique: group data Items into classes with similar characteristics to maximise or minimise interclass similarity- for example, to identify suspects who conduct crimes in similar ways or distinguish among groups belonging to different gangs (Chau, Xu & Chen, 2002).

c) Deviation detection: researcher deploy this technique to detect fraud, network intrusion detection, and other crime analysis that involve tracing some activities which can be appear sometimes to be abnormal.

d) Classification: finds common properties among different crime entities and organises them into predefined classes. This technique has been used to identify the

source of email spamming based on the senders linguistic patterns and structural features.

e) Social network analysis: describes the roles of and interaction among nodes in a conceptual network. Investigator can use the technique to construct a network that illustrates criminal's roles, the flow of tangible and intangible goods and information (Chau, Xu & Chen, 2002).

In 1990 the profiler Brent Turvey met with and interviewed an incarcerated serial killer after extensively reviewing crime report, court transcripts, and court records. Nothing matched, Turvey could not comprehend how the prisoner's statement could be so contradictory to the information in the crime reports until he realised that the perpetrator was purposely misconstruing the facts to redirect the responsibility of the crime. Turvey felt it was more reliable to look at the forensic evidence and then using the criminal event, to reconstruct the behaviour, (Rogers, 2003).

The question of why some people commit crime is a subject which has presented criminologists and sociologists a challenge for many years, and, like many such questions, is one to which there is no simple answer, [2,5]. Johnson(2005), (Johnson, 2005), have done some fine preliminary work developing typologies, classifying the serial computer criminal as crucial in determine the underlying motivating causal factors. Classification is made by assessing and analysing the written, physical, and digital behaviour that exist in each attack. Any understanding of crime patterns and offenders motivation should start perhaps with the question of why people commit crime in the first place. Profiling has traditionally been thought of as attempting to reduce the number of possible offenders to the point where traditional methods of investigation can be introduced to solve the case (Ainsworth, 2001). Interpreting the intrusion from the criminal point of view will greatly assist the investigator in understanding what motivates an offender, (Johnson, 2005).

In the case of cybercrime as there is a rapid change of the technology, therefore, cyber criminal's behaviour may become dynamic. This change in behaviour will require a reclassification of the typology being currently used. Essentially, cyber criminal's behaviour is evolving and changing overtime with experience where they learn from their actions, or from their friend's experience, which will enhance their skills. The offender signature which is a repetitive ritualistic behaviour that the offender usually displays at every crime scene provides police an appropriate profiling tool, (Johnson, 2005). This will give the investigator the opportunity to understand the motivations that drives the offender to perpetrate such crime. This finding will result in assisting the researcher in the classifying of the type of perpetrator that is being sought.

It is important that we consider some of the more prominent theories of criminal behaviour if we are to understand trends and patterns in criminal activity and if we are

to understand the behaviour of those sought by profilers. It would be naive to presume that the reason why most people commit crime can be found in just one theory (Ainsworth, 2001). However, the choice of which profiling method to use is controversial. On the surface, it appears that deductive profiling is more suited to computer-related cases than using inductive profiling methods such as the FBI or IP method, which are culturally biased and does not make practical sense, (Rogers, 2003).

Deductive profiling methods (e.g., Behaviour Evidence Analysis (BEA)), unlike the FBI or IB methods, do not rely on a large offender database or on statistical analysis of previously convicted offenders and should be less culturally biased (Rogers, 2003). BEA was developed by the profiler Brent Turvey, in order to overcome some of the FBI and Investigative Psychology (IP) models, (Rogers, 2003; Turvey, 2002; Nykodym, Taylor & Vilela, 2005). The BEA method has four steps and two primary phases which includes Victimology and Computer Scene Characteristics.

Conclusion

Researchers academically or commercially are continually creating filtering and search engines to find and sort documents from multiple resources. Criminals use zero day vulnerabilities to get what they want and anti-forensics techniques to cover their tracks.

Despite a plethora of Internet related legislation, cyber crime is still a growing stigma for the e-society. It is evident that Internet usage requires laws and regulatory authorities, which should span across national boundaries and legal systems.

References

Ainsworth P.B., (2001). Offender Crime Profiling and Crime Analysis. USA and Canada, Willan Publishing.

Broadhurst, R. And Chantler, N., (2006), United Nations Office on Drugs and Crime: Cybercrime Update:Trends and Development online, http:// www. eprints. qwt. edu.au/archive/00004690

Broucek, V., and Turner, P., (2006), Winning The Battles, Losing The War?, Rethinking Methodology for Forensic Computing Research. Journal in Computer Virology 2(1) pp.3-12.

Chau, M., Xu, J., & Chen, H., (2002). Extracting meaningful entities from police narrative reports. In: Proceeding of National Conference for Digital Government Research (dg.o 2002), Los Angeles, California, USA.

Johnson, T. A., (2005). Forensic Crime Investigation. USA, CRC Press.

Kanellis P., Kiountouzis E., Kolokotronis N., and Martakos D., (2006). Digital Crime and Forensic Science in Cyberspace, Idea Group Inc. (IGI), USA.

Leyden, J. (16 October 2006). Brits in their Identity as ID thieves prosper. The Register Magazine.Available at http://www.theregister.co.uk /2006 /10/ 16/id _fraud_ prevention_week /. (Accessed August 2007).

Nykodym, N., Taylor, R., Vilela, J., (2005), Criminal Profiling and insider cybercrime. Computer Law and Security Report 21(5), pp. 408-414.

Rogers, M., 2003, The role of criminal profiling in the computer forensics process. Computer & Security 22(4), pp.292-298.

Turvey, B., (2002). Criminal Profiling, An Introduction To Behavioural Evidence. UK, Elsevier.

Wilson, R. 2006, Understanding the Perpetration of Employee Computer Crime in the Organisational Context. Working paper no.04-2006.