Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Data attack of the cybercriminal: Investigating the digital currency of cybercrime

Paul Hunton

Hunton Woods Limited, UK

Keywords:
Cybercrime
e-Crime
Internet Crime
Hi-tech Crime
Cybercriminal
Police
Policing
Law enforcement investigation
Digital investigation

ABSTRACT

It is increasingly argued that the primary motive of the cybercriminal and the major reason for the continued growth in cyber attacks is financial gain. In addition to the direct financial impact of cybercrime, it can also be argued that the digital data and the information it represents that can be communicated through the Internet, can have additional intrinsic value to the cybercriminal. In response to the perceived value and subsequent demand for illicit data, a sophisticated and self-sufficient underground digital economy has emerged. The aim of this paper is to extend the author's earlier research that first introduced the concept of the Cybercrime Execution Stack by examining in detail the underlying data objectives of the cybercriminal. Both technical and non-technical law enforcement investigators need the ability to contextualise and structure the illicit activities of the cybercriminal, in order to communicate this understanding amongst the wider law enforcement community. By identifying the potential value of electronic data to the cybercriminal, and discussing this data in the context of data collection, data supply and distribution, and data use, demonstrates the relevance and advantages of utilising an objective data perspective when investigating cybercrime.

1. Introduction and background

As the Internet continues to grow and rapidly transform many aspects of modern life, the benefits and opportunities afforded by a globalised digital society are arguably immense.

However, as networked communication technologies continue to evolve and increasing reliance is placed on the extensive range of functions and services on offer, individuals, organisations and governments alike are increasingly exposed to the risks and threats of the cybercriminal. As a consequence of this vast digital freedom, the Internet also offers the motivated and organised cybercriminal new and innovative opportunities to commit a vast range of repeatable illicit activities against a global community with near anonymity (Bryant, 2008; Fletcher, 2007; Hoare, 2010). Daily examples of cyber related crimes are demonstrated by such offences as: fraud; identity theft; theft of intellectual property rights; money laundering; online grooming; cyber-bullying; pornography and paedophilia. The concept of cyber security extends this virtual threat even further when considering such illicit activities as cyber terrorism and cyber warfare, industrial espionage and disinformation ranging from information warfare to propaganda and political attack. It is now argued that terrorists and extremists are utilising the content rich interactivity of the Internet with the same level of technical sophistication as national governments (Qin et al., 2007).

Already highlighted by the author elsewhere (Hunton, 2009, 2010), are the many common issues and challenges faced by the global law enforcement community when investigating the complexity of cybercrime. These challenges include: under reporting of technology crime; potential for mass and globally spread victims; the issue of jurisdiction; evidence acquisition of distributed and volatile technology; evidence presentation; pace of changing technology; and the

0267-3649/$ – see front matter © 2012 Paul Hunton. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.01.007

need for investigators to continually develop and maintain adequate technical skills and knowledge. The evolving state of technology is a major challenge for law enforcement, as the dynamics of a specific technology environment become understood, that environment can again quickly change (Mitchell et al., 2010). Furthermore, the concept of cyber criminality is often clouded by the interchangeable, inaccurate and even contradictory terms commonly used to describe the vast array of illicit activities and behaviours associated with cybercrime and cyber security (Bryant, 2008; Sommer and Brown, 2011; Wall, 2007). However, cybercrime is now considered a very real and serious global issue by many nations and a problem that has evolved to become a sophisticated transnational threat operating on an industrial scale (Cabinet Office, 2009; Commonwealth of Australia, 2010; Cyberspace Policy Review, 2009; e-Crime Congress, 2009; Finklea, 2009; New Zealand Police, 2009).

Therefore, the aim of this paper is to extend the author's earlier research that first introduced the concept of the Cybercrime Execution Stack (Hunton, 2009) by examining in detail the underlying data objectives of the cybercriminal when attempting to execute cyber attacks. By identifying the intrinsic value of electronic data to the cybercriminal and by discussing this data in the context of: data collection; data supply and distribution; and data use, is aimed at demonstrating the advantages and relevance of utilising an objective data perspective when investigating cybercrime. The final outcomes from this discussion are intended to provide additional insight into how the initial complexity of a cybercrime investigation can be broken down, the outcomes used to directly assist understanding and knowledge sharing, and also influence and support further investigative enquires by both technical and non-technical investigators.

2. The digital currency of the cybercriminal

It is increasingly argued that the primary pursuit of the cybercriminal and likewise, a major factor for the continued growth in cybercrime is financial gain (Choo and Smith, 2008; Commonwealth of Australia, 2010; Kapitanskaya, 2010; Maple and Phillips, 2010; Symantec, 2009). The growing problem, and the financial motivation behind cybercrime, can be demonstrated when considering research in the Garlik (2009) UK cybercrime report that suggests between 2007 and 2008 in the UK alone 40% (86,900) of all identity fraud was facilitated online. Again, during this period, online UK banking fraud increased from the previous year by 132%, totalling £52.5 million fraudulently obtained, and card fraud that took place on the Internet accounted for a further £181.7 million in losses (Garlik, 2009). The UK government now suggest that the impact of electronic crime on the economy is running into billions of pounds annually (Cabinet Office, 2011), and that the wider global impact is now calculated at $1 trillion per year (HM Government, 2010). From a UK law enforcement perspective, cybercrime is considered to be one of the biggest threats to the country's economic future well being (Orde, 2011).

Fundamental to all communication and interaction across the Internet and other networked technology is electronic data and the information it represents. Therefore, like any essential commodity, electronic data in addition to the immediate use and direct financial impact in crime can also be argued as having a wider intrinsic value to the cybercriminal. This additional value can be realised based on the opportunities it represents to other criminals. Unlike a single physical criminal activity that results in monetary gain, online crime has the potential to be repeated numerous times to commit such illicit activities as: online-banking transfers; credit card purchases or accessing secure networks. In response to the demand and subsequent value placed on illicit data, a sophisticated and self-sufficient underground digital economy and marketplace has emerged (Cisco, 2010; DeBolt, 2010; Europol, 2011; Symantec, 2009, 2010b). These digital criminal markets can be seen to facilitate the direct financial gain from the: collection; sale; distribution and use of illicit data and the subsequent information it represents. Examples can include notorious sites and forums such as Darkweb, Ghostmarket, Maza and Direct Connection that when exposed where found to be conducting illicit trade with business like scale, professionalism and coordination. The underground trading of illicit data can include sensitive personal identity details, credit card and online account credentials through to intellectual property theft covering business data and even industrial espionage (Symantec, 2008, 2010a). Further examples of the cybercriminals profiteering from the supply and demand for illicit data can also include digital copyright infringement covering the distribution of eBooks, software applications, music and videos through to the more depraved and sinister issue of paedophilia and pornography.

Knowledge and skills that can be used in an illicit context covering technical details such as system weaknesses, predefined attack scripts and purpose built crimeware toolkits are also data driven and widely available at a cost within the context of an underground illicit marketplace. In addition, to support the conversion of digital currency into real-world profits, other services surrounding money laundering and the use of 'money mules' are also increasingly available (Cisco, 2010). Symantec (2009) estimate an average value for the potential opportunity for fraud, based on the many datacentric goods and services offered for sale by cybercriminals on the Internet, to be over £3.5 billion. Although many of these online criminal markets are concealed from public view, others are just discreetly placed amongst the numerous legitimate Internet resources and can be found using a conventional search engine or by following the discussions and links on social networking sites; online gaming and other Internet community forums.

3. Data attack of the cybercriminal

A cybercriminal's ability to use technology and exploit the Internet to directly access, manipulate and communicate electronic data is a basic feature in the commission of cybercrime and other illicit or criminal behaviours. Internet related technology can be used to commit crime either entirely within a technical environment, or to facilitate conventional crime by using various elements of networked technology. Regardless of the extent of networked technology used in the commission of cybercrime, the common technical activities of the