The Role of the Refrigerator in Identity Crime?

Eric Holm
Federation University Australia
P.O. Box 668, Mount Helen 3353
e.holm@federation.edu.au

ABSTRACT

This paper explores how botnets in smart devices are exacerbating identity crime. This paper places the refrigerator at the heart of this discussion of the Internet of things that has become connected through the Internet and thereby susceptible to botnets and the collection of personal identification information as an enabler for identity crime. The paper highlights the fallibility of these devices and provides some mechanism to deal with these new risks and presents discussion on the need to for this relationship to be further explored.

KEYWORDS

Botnet, computer crime, identity crime, identity theft, Zeus botnet.

1 INTRODUCTION

Botnets are connected computers communicating across the Internet to complete various tasks and have become common in many acts including having become known through their association with denial-of-service attacks [1] and with the distribution of spam [2]. To commit these types of actions, botnets remain concealed in a victim’s computer and take commands from their master while stealthily spreading themselves across the Internet [3]. The term ‘botnet’ is an amalgam of two words, namely the ‘robot’ and the ‘network’ [4]. The robotic feature of the program relates to the autonomous nature of the software and the network and the pathway for them to be disseminated [4]. The use of botnets has expanded to incorporate many crimes and the criminality surrounding them is evolving [5].

Not all botnets are bad botnets; for instance good botnets are used by search engine providers such as Google to improve their search engines [3]. These improvements are positive for end users and certainly enhance the ways in which the Internet is used [3]. However, at the same time, botnets are widely known for inflicting harm through their potential for use in activities, some of which are criminal [1], [2]. What makes botnets dynamic is their ability to be customized by programmers for a variety of purposes that can include both criminal and non-criminal acts. For this reason, they can inflict widespread damage through criminal acts, particularly as they can spread themselves across the Internet. In this way, they have become recognized as a pandemic to the security of the Internet [6]. The Zeus botnet is an example of a widely known botnet that is used for stealing individual and corporate credentials [7]. The Zeus toolkit has historically infected millions of computers in the United States and worldwide [8].

2 WHAT DOES THE BOTNET DO?

The primary role of the botnet is to function according to the programmed instructions it obtains, and to report back to the bot-master (the person in charge of the botnet) [9]. The master of the botnet provides commands that direct the many actions of the botnet. In following these instructions, the botnet will routinely check with the master for new commands [10]. The programming of commands from the bot-master thus define the scope of criminal activities undertaken. The control is understood to entail ‘command and control’ which is a phrase used to express the dual function of the bot-master in controlling the botnet in the way desired while also adapting this control as desired through
command [9]. The overwhelming strength of a botnet attack comes from the coordination of computers co-opted for the purpose and as the number of computers increases, the army becomes larger and the associated threats to the controlled computers increase [9]. Through this process, the botnet aims to remain concealed within devices connected on the Internet to avoid detection [11] and accepts these instructions to operate in ways that are remote and also cover which support the primary role of the botnet [12].

The adaptability of botnets makes it possible to configure their use for identity crime; the impetus for this activity is about using the botnet for the collection of personal information as the catalyst to committing identity crime [12]. Under Australian criminal law, unauthorized dealing with personal identification information is a key aspect of identity crime [13]. Central to the crime is the possession of and dealing with personal identification information which includes people’s dates of birth and their full names and addresses, but is not limited to these [13]. For the crime to apply, this information must be used or dealt with [13]. In this way, information has value when considered according to its propensity for misuse [14]. Accordingly, the value of this information depends on what can be done with it, but the mere possession of such information is regarded as an offense, for instance under the Australian Commonwealth Criminal Code [13].

Botnets can be created with a relatively low level of technological skill and the skill utilized to develop these will vary according to the skills of the person creating them [15]. Consequently, the broader market for criminal “services” online, to be used for cyber-crimes, also continues to grow [15]. For instance, services to develop botnets are becoming more prominent as is the provision of botnets to order, such as for the purposes of denial-of-service attacks or to spam [16]. The level of sophistication of the botnet varies as does the level of obfuscation based on their design and implementation [6]. As a consequence, the market for the development of services supporting the development of criminal services is increasing as is the level of sophistication generally.

One aspect of botnets that differentiates their creation from other acts is that they are relatively inexpensive to create and manage for a variety of purposes whether legal or not. They are often sold as customizable toolkits, and in this way, the customization provides for adaptability [17]. Starting from a base line of a Zeus botnet, the adaptation of botnets serves a number of functions, including the collection of personal identification information and tracking online behavior patterns [18]. The botnet can readily be adapted for undertaking a variety of actions including those that could be used to facilitate identity crime [19]. A consequence of this is that botnet activity might result in myriad criminal offenses linked to identity crime as well as other crimes [8]. The Australian Institute of Criminology has identified that botnets play a significant role in the promulgation in phishing attacks and their adaptability makes them into a tool of crime [20]. Compounding these features is the pervasive nature of botnets and the ability to use them to facilitate coordinated mass attacks across the Internet [21]. The botnet army obtains strength from its size and scale, and it can be enormous [21]. In this respect, the pervasive nature of the crime coupled with the customization of the botnet is what makes this tool unique if used for crime [8].

The refrigerator has been used in this article to illustrate how an innocuous device, namely the household refrigerator, can be used to perpetrate offenses relevant to identity crime through botnets. The refrigerator can only be used for the distribution of botnets if it is ‘smart’ and what makes a device ‘smart’ is its web enabled interoperability [22]. Increasingly, domestic household appliances have Internet connectivity and thereby have progressively become ‘smart’ and consequently potential targets of botnet attacks [23]. ‘Smart’ devices include tablets, computer routers and switches, among others [24]. The attractiveness of these devices as targets for botnets stems from the extraordinary number of devices connected to the Internet [24] and the technological security weaknesses these devices have [24]. Mobile smart devices tend to have
infrequent updates and lackluster security measures [25]. Smartphones for instance, have become vulnerable to botnet attacks for many of these reasons [26]. Eslahi, Salleh and Anuar have referred to these botnets as MoBots as they operate through mobile devices and through the use of mobile networks [25]. Damballa Research Laboratory in 2011 indicated that up to 40,000 infected computer systems were detected within the first six months of that year [27]. These devices add to the bulk of compromised systems and potential armies that can be involved with botnet activity. Accordingly, these contribute toward the spread of risks associated with botnets and their related crimes [28].

The phrase ‘Internet of things’ is used to explain how so many devices or ‘things’ are interoperable with the internet [12]. The Internet of things expresses the interconnection on the Internet of everyday objects including those mentioned that share this space [12], [29]. These devices share an affinity through the extent they interoperate on the Internet but also by the ways they could contribute to the armies of remote controlled computers connected to the Internet. In this way, the innocuous kitchen device, the ‘smart refrigerator’ can now play a clandestine role in perpetuating identity crime. On the vulnerability of these devices on the Internet of things, Hewlett-Packard suggests that around 70 per cent of devices connected to the Internet have vulnerabilities [30]. This means that a significant number of devices could play a role in botnet distribution. The most notable problems for many of these devices is the lack of encryption, the ease of access, and the absence of security measures such as the use of passwords which facilitate their use in this way [30]. Furthermore, a problem with these devices is that there is no easy way to install an antivirus or related security mechanism, which also applies to most refrigerators [30].

3 EXAMPLES OF BOTNETS

An example involving a refrigerator, television and home router being used in a botnet attack in Australia occurred in 2014; they were found to have sent 750 thousand malicious emails [31]. However, a number of other examples of botnet attacks have been known to have a far more profound impact. A key example of a major botnet attack in Australia was the Citadel, a botnet that targeted banking credentials and this was responsible for losses amounting to the equivalent of more than US$100 million [32]. The Citadel botnet attack identified where financial information was entered by a computer user and would then extract that information for the purposes of committing fraud [33]. The impact of this crime was profound in Australia, with over 30,000 detected instances of infected computers infected in Sydney alone. The overall losses attributed to this botnet alone have been estimated at over A$500 million dollars [33]. The Gameover Zeus botnet similarly compromised over 75,000 computers and compromised more than 2,500 international organizations [34]. The efforts to disrupt this botnet were only possible due to a multinational effort that took place to investigate offenders [35]. The Federal Bureau of Investigation suggested that this botnet attack was one of the more significant attacks of its type that they have investigated, due to the worldwide infestation [32], [34]. Indeed, the harm caused by botnet attacks is difficult to measure based on their size in isolation, but harm can be measured by considering both the respective size and reach of a botnet. For example, by using a botnet comprised of 183,000 zombie devices, criminals harvested 310,000 items of identity including 310,000 bank account details, credit card details as well as social networking credentials [36].

4 CAN THE REFRIGERATOR BE USED FOR IDENTITY CRIME?

The refrigerator itself cannot be a criminal; for the purposes of identity crime a refrigerator is not a natural person and cannot possess the ‘intent’ to commit a crime [37]. Likewise, it is difficult to assert that the botnet is the criminal as similarly it cannot possess that intention to commit a crime. Rather, the refrigerator can be an instrument of crime under certain circumstances. In this regard, the refrigerator is a resource that can be used to facilitate a crime, but it is dependent on the intentions of the criminal. Symantec provides an
example of this where a criminal used a refrigerator to send 100,000 spam through an installed botnet [38]. Hence, rather than the refrigerator or the bot being the criminal, it is the person in control of the botnet that has the criminal intent. To perpetrate the crime, the refrigerator and the botnet are used together to enable identity crime.

Identity crime is defined by the Organisation for Economic Co-operation and Development (OECD) as a crime where one party uses the personal information of a person in an unlawful manner [39]. Key to establishing an identity crime is to establish the possession of or use of personal identification information [13]. Within the literature, a distinction has been drawn between identity theft and fraud, to delineate cases in which the theft involves only the theft of identification information and where it involves fraud [40]. This is despite the fact that one action, the theft of information, is often the catalyst for the other, the fraud associated with the theft. Common to any allegation of identity crime is the unlawful use of stolen information, typically with the view to obtaining some advantage which might relate to fraud, but does not always need to [40]. The European Network and Information Security Agency similarly suggests that common to the perpetration of cybercrimes is the desire to extract credentials for some gain [41].

In relation to specific crimes pertaining to this, identity theft is an offense if one’s identity is obtained and is possessed wrongfully [42]. As discussed, the criminal offense is the unlawful use of another’s personal information [43], and many concede this as the basis for the establishment of their crime. It should be noted that Australian states and territories construe the laws relating to this crime slightly differently from each other, and there are considerable variations in the punishments associated with committing these offenses. Penalties vary from five years’ imprisonment upon conviction, but up to ten years’ imprisonment is possible in some states / territories [44]. Similar contrasts can be made between the penalties for offenses when comparing Australia and other countries, notably the United States [45]. Furthermore, whereas identity crime is recognized as a crime in most Australian localities, in some countries it is not thus recognized in all, and this results in disparities with respect to offenses and penalties. This disparity challenges the consistency of offense penalties applied, but this discussion falls outside the scope of this paper.

In Australia, the use of a botnets to facilitate crime is covered by criminal offenses that include those relating to access [46], interference [47], and misuse of devices [48]. These are offenses that symbolize the nature of undesired and undesirable behavior. The punishment commensurate with the crime(s) is often determined by considering the offenses committed. For the purposes of this paper, assuming the requisite elements of the unauthorized modification of data are satisfied, then this can have a penalty of up to 10 years’ imprisonment [47]. Likewise, the offense of the unauthorized impairment of electronic communication carries similar penalties [49]. Further, if a botnet is involved with the dissemination of spam and phishing this will attract different or further sanctions [50] and this is plausible as a relationship can exist between spam and phishing. Indeed, if this crime is directly linked to that of identity crime, then in absence of aggravated provisions, the compounding penalties of the offenses listed would apply.

5 INDICATORS OF THE CRIME

Many users remain unaware of the presence of botnets on their devices [3]. There can be difficulties in detecting botnet activity, particularly when they are designed to remain concealed. Further, the evolution of different platforms has increased the difficulties of detecting the warning signs that a botnet is present [51]. Another challenge in the detection of botnet attacks is that botnets reside differently depending on their customization and dissemination [25]. The determination of location is particularly challenging for mobile devices as they can be used anywhere [52]. Having stated these difficulties, the United States Federal Bureau of Investigation states that there are a number of indicators that make it evident that a computer has been infected
by botnets [35]. Common warning signs include system slow-downs related to high levels of disk activity [35], [3]. However, the indicators of identity theft are far more difficult to identify. Interestingly, governmental bodies in the United States remain well placed to provide commentary on identity crimes, particularly as they remain prominent and public there. The United States Federal Trade Commission proclaimed in 2013 that identity theft was the most common national consumer complaint [53].

In responding to this crime, there are often delays in its detection by victims, and this complicates the information known about the crime [11]. Investigation can be hampered by the time lapse between the identity crime occurring, and its being reported [53]. Because of this delay, the perpetrators have ample opportunity to avoid apprehension [36]. Law enforcement agencies are similarly impeded due to the geographic dispersion of these crimes particularly where the identity crime has a relationship with botnets [54]. The Internet provides many criminals with anonymity and the jurisdictional problems faced with the geographic reach of these crimes impact on the ability of law enforcement agencies to respond [55]. Delays in detecting the crime adds to the complexity of responding to the crime [56] and complicate the ability of law enforcement agencies to deal with the crime in a timely manner [57]. Identity crime itself can be a crime that can be difficult to detect [58] and a part of this problem is that mostly the crime is eventually detected by the individual, but not usually until the individual detects unauthorized transactions [59]. The botnet is designed to be elusive and due to this characteristic, it too makes the detection and responses to it difficult.

6 THE NEED FOR DATA AND RESPONSES

Information can be a barrier to understanding crime and this exists for many cybercrimes [60]. While there are bodies that are well placed to collect information relevant to these crimes, often the data relevant to crimes are construed narrowly and certainly seldom shared [57]. The sharing of knowledge related to these types of emerging crimes needs to be improved so that this crime and others like it can be better understood [42]. In addition, a repository of information related to the crime will invariably assist all relevant stakeholders in understanding the prevailing risks from this crime [42]. In this regard, governments can play a role in collecting data in relation to this crime as they can also play a role in disseminating data relevant to it.

Governments play a key role in the responses to crime as they can ensure coordinated efforts are made through relevant stakeholders and constituents. These crime control measures are needed so that governments, international bodies, ISPs as well as other stakeholders work together as they are all impacted in some way by these crimes [61]. The coordination imperative is complicated by the many different agendas that exist for each of these parties [61]. In this regard, there are barriers to achieving this, namely around sovereignty but also by competing agendas [61]. Nevertheless governments play an important role in dealing with the development of strategic and policy responses to these emerging crimes which are critical to influencing regulatory responses as well as other responses [62]. In particular, there is a need for better coordination between government and industry in relation to responses to these crimes [63]. It is hoped that a greater awareness of the risks associated with these newly emerging variants of crime will prompt the actions of government needed to deal with these crimes.

Regulatory responses to crime need to be better defined to match the risks that the crime presents. In the absence of data on this, responses can be difficult. There can be some difficulties in capturing new offense variations such as those discussed here, due to the ways that legislation is currently constructed. Whereas regulatory responses can be drafted narrowly, they can fail to capture the desired criminal behaviors as they are applied intently. Alternatively, they might be drafted broadly and consequently become diluted, which is problematic as they then fail to be specific enough to capture the criminal activities intended [64]. The difficulty in calibrating appropriate regulatory responses is to find a
balance between regulations that are tight enough to capture the necessary variations of offenses, but loose enough to deal with the varieties of crime. Beyond the original drafting of legislation relating to these offenses, the responses to crime need to have some flexibility to adapt to newly emerging variations of offending. It is for this reason that the regulatory responses have be adaptable to encompass the challenges presented by these crimes [57]. At present, this remains problematic as the offending associated with identity crime and botnets has no universally accepted offense or definition. Whereas this requires some dynamism in the application of criminal sanctions for related offenses, it also presents motivations for the laws to be further developed.

Any response to this crime will also require a collaborative international effort due the crime’s multi-jurisdictional nature [41]. A necessary precursor to dealing with these problems is the harmonization of laws related to the crimes at an international level [41]. Within the international mechanisms that promote harmonization of cybercrimes, there is little coverage of identity crime and botnets [65]. Having said that, it would be plausible for these offenses to be subsumed or captured within related offenses. Further, a positive benefit of international agreements relating to cybercrime is that they foster the development of domestic responses to related offenses [60]. However, more development of the law, particularly to facilitate harmonization, is needed for crimes that straddle jurisdictional boundaries and offense types.

A better understanding of the relationship between individuals and technology vulnerabilities would also increase the stringency of responses. Behavioral factors are multifaceted and need to be better understood particularly as humans remain (in a general sense) a known weakness in cyber security [26]. This weakness has relevance to both botnets and identity crime insofar as these crimes are linked together often by the fallibility of human behavior. Despite many of these already having been investigated, a further insight into these in the specific context of identity crime and botnets will fuel the development of preventative steps needed to address the risks by focusing on the behavioral problems [62]. However, at the same time, there is an arms race between those that wish to protect information and those that are looking to exploit it [55]. Nonetheless, as the techniques to deal with bots and identity crime from a behavioral perspective evolve, so do the many ways of working around technological solutions to prevent these risks [2]. For this reason, it is important that the preventative steps supersede the actual risks.

Technological responses to crimes also provide for ways of dealing with crime through non regulatory means. Technological responses provide another way of understanding how these crimes can be responded to, with measures such as filtering, blocking and blacklisting as select example of ways of preventing such attacks from taking place [41]. Technological responses like encryption and authentication also provide for ways of preventing identity crime, although the direct relationship between these preventatives and the crime are not definitive [57]. Indeed, some technological responses operate to complement regulatory and other responses but because these crimes are both pervasive and adaptable, the responses to this crime also need to be dynamic [61]. Indeed, as methods to perpetrate identity crime emerge, so do the technological methods that overcome them and for this reason an increased focus on the development of technological responses is needed. Whereas technological responses to any cybercrime are not a panacea to resolving this type of crime, they provide ways of dealing with the crime in ways other than regulation [41]. These responses to crime can play an important role in reducing the incidence of botnet attacks as well as identity theft [42]. In respect to the adoption of approaches other than regulation, the benefit of multiple approaches to dealing with crime is that broader policy objectives underpinning their existence can be met [39].

7 DISCUSSION AND CONCLUSION

The emergence of smart devices has contributed to the Internet of things which represents a conglomeration of devices connected to the
Internet. These devices, which include the smart refrigerator, provide mechanisms through which botnets can operate and if appropriately customized, can gather the information needed for identity crimes to be perpetrated. In this way, this paper has deliberated on how the botnet could have a positive impact on the occurrence of identity crime through these types of smart devices. The paper places the refrigerator at the heart of the discussion as a smart device that plays a role in botnet attacks, using this smart device as an exemplar to highlight how the botnet could be infiltrating this innocuous device due to their lackluster preventative measures.

The paper explored responses to botnets and identity crime and presented a discussion about the challenges of operationalizing these. The paper contends that whereas these crimes are considered separately from one another, the relationships between them have only rarely been considered. Lastly, the paper provides some options for dealing better with identity crime and underpinning these is the need for more research to be undertaken to understand how botnets share relationships with crimes like identity crime.

8 REFERENCES


44. Commonwealth Criminal Code Act 1995 (Cth), Division 372.1

47. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 477.2.
49. Commonwealth Criminal Code Act 1995 (Cth), Division 477, Section 477.3.
50. Spam Act 2003 (Cth) Section 5.