Mitigating Botnet Information Security Risks through Enterprise Architecture and the Information Technology Security Architecture

Christopher Furton

Syracuse University

Abstract

This paper investigates the threats of botnets to the enterprise environment. First, this paper looks at the history of botnets and the evolution of command and control topologies. Propagation techniques are reviewed as well as analysis of advanced botnets that target enterprise information systems. The use of botnets is analyzed resulting in a list of 19 botnet risk area topics that, if unmitigated, can be devastating to the organization's business processes. Next, this paper examines mitigation activities, namely the Information Technology Security Architecture model (Bernard & Ho, 2008), that can help organizations reduce the possibility of botnet infection and reduce the impact if an infection occurs. Lastly, this paper presents a case study where a nation-state uses part of the business continuity planning process of the Information Technology Security Architecture to mitigate a distributed denial of service attack.

Mitigating Botnet Information Security Risks through Enterprise Architecture and the Information Technology Security Architecture

Often referred to as zombies, malware compromised computers take part in criminal cyber activity without the knowledge of their owners. Zombies are members of large networks called Botnets. These networks range in size and complexity, but all have serious implications to enterprise security. As a tool for criminal activity, botnets can 'earn' criminals substantial revenue by engaging in spam mass emailing and information theft campaigns. Similarly, some criminals generate revenue by renting access to their botnets to other cyber criminals (Ferguson, The history of the botnet - Part II, 2010). Besides financial gain, botnets are a common tool for hacktivism where hackers use malicious attacks to further a political viewpoint (Schectman, 2012).

This paper explores the world of botnets. The paper is broken into four parts: 1) The Problem; 2) The Mitigation; 3) The Case Study; and 4) The Conclusion. In 'Part 1- The Problem', the goal is to explain the types of technologies utilized in botnets and identify the potential risks associated with them. In 'Part II – The Mitigation', the goal is to offer recommendations for combating botnet risks specifically through the use of proven methodologies such as the Bernard & Ho's Information Technology Security Architecture (2008). In Part 3 – The Case Study, a real life look at a nation state that used business continuity planning to reduce the impact of a botnet distributed denial of service attack. In 'Part 4 – The Conclusion', the goal is to tie the main points of this paper together.

Part I – The Problem

This section of the paper provides background information on botnets and identifies the problems faced by internet users and the enterprise environment. The contents include: a brief

technical overview, explanation of propagation techniques, topology differentiation for command and control, discussion on intended targets, typical use of botnets, and the history of botnets. The aim of Part I is to ensure an understanding of botnets and introduce the problems that they cause to the enterprise environment.

Botnet Technical Overview

To help understand the risks of botnets to the enterprise environment, a technical understanding of botnets is essential. "Botnets are proving to be the most recent and disastrous threat to the field of information technology" (Naseem, Shafqat, Sabir, & Shahzad, 2010). Botnets come in many different sizes and structures, but all of them have potential to cause significant damage to the enterprise environment. As shown in the history section, botnets have been around for a significant amount of time and are constantly evolving with technology.

The first step to understanding how to mitigate botnet risks involves learning and understanding the lifecycle of a botnet. As discussed by Naseem et al. (2010), a botnet attack begins by exploiting vulnerabilities in user computers. These vulnerabilities provide the attacker, referred to as the Botmaster or Botherder, with an entry point to a system to install malicious software. Once the botmaster has installed the software, the computer is now a 'bot' or 'zombie' which can be used to execute attacks or continue spreading (Naseem, Shafqat, Sabir, & Shahzad, 2010).

One unique aspect of botnets typically unseen by other forms of malware is the command and control (C&C) channel. The communication mechanism behind this channel varies depending on specifics of the botnet, however, all are used to control the activities of the bots, issue commands, and accomplish the botmaster's agenda. Once this communication channel is detected, the whole botnet maybe exposed (Naseem, Shafqat, Sabir, & Shahzad, 2010).

As technologies evolve, botnets have also evolved communication methods. As mentioned in the History section, early botnets often used IRC channels for command and control. Further evolution developed into peer-to-peer and web traffic (hypertext transfer protocol) command and control channels (Naseem, Shafqat, Sabir, & Shahzad, 2010). In today's Internet, other communication mechanisms are becoming common. Botnets have been detected that utilize the popular Twitter social networking website for C&C activities (The H Security, 2011). Furthermore, researchers have developed a theoretical covert social network botnet that embeds C&C messages into images uploaded to the Facebook website. This proposed botnet "use[s] image steganography to hide the presence of communication within [an] image" (Nagaraja, Houmansadr, Piyawongwisal, Singh, Agarwal, & Borisov). A more detailed discussion on botnet topologies can be found in the subsequent section on 'topology.'

At face value, a botnet sounds similar to a virus or worm. However, one significant difference that puts botnets into a category of their own is the botmaster's ability to control compromised computers (Naseem, Shafqat, Sabir, & Shahzad, 2010). Traditional malware may perform similar functions as a botnet, however, the propagation is not controlled in the same way that botnets are. By design, botnets are stealthy and covert malware with potential to cause substantial damage to an organization's enterprise environment. Preventing infection and reducing the propagation of botnet malware is key to protecting the infrastructure.

Propagation Techniques

In order to discuss propagation techniques, it is first important to clarify that botnets are a network of compromised hosts. Developing a botnet occurs by infecting vulnerable computers with command and control malware giving the botmaster control of the newly created bot.

When discussing propagation techniques, this paper focuses on activities used by botmasters to initially infect vulnerable computers.

In the beginning stages of propagation, botnets look for vulnerable hosts that have unpatched operating systems or software applications. The methods used to exploit these vulnerabilities are often controlled by the botmaster during propagation. Successful botnet propagation relies on a controlled rate of infection that doesn't interfere with network stability. Too rapid of propagation can result in network instability and reduce the overall effectiveness of the botnet (Xin-liang, Lu-Ying, Fang, & Zhen-ming, 2010).

In contrast to the preferred controlled propagation, some botnets spread similar to malware worms. In these instances, an already compromised host finds other vulnerable hosts and exploits them without influence from the botmaster. This form of propagation is wild and uncontrollable.

The propagation methods discussed above do not require user interaction. However, many botnets propagate in a matter that requires a user to perform a task. The first and most common method (Dagon, 2005) of propagation is by email. As seen in mid-2011, the ZeuS botnet used email to spread in the form of a fake IRS spam email. In this example, the emails appear to originate from the irs.gov domain where the subject reads "Your IRS payment rejected" or "Federal Tax payment rejected." The body of the email refers the victim to an attached PDF file containing the ZeuS malware (MXPolice, 2011). Using social engineering tactics (the fear of IRS audit), the ZeuS botnet leveraged email as a method for propagation.

Another propagation method is through instant messaging. In this method, botmasters attempt various forms of attack through instant messaging including social engineering attacks attempting to lure the victim into clicking a malicious link. Additionally, the botmaster can send

a malicious file to the victim and entice him/her into opening it (Dagon, 2005). As seen in the Mariposa botnet, which was shutdown in March of 2010, the instant messaging software MSN Messenger was used by threat actors to spread malicious code to unsuspecting victims (Kolakowski, 2010).

Web pages are also often used to spread malicious code that enables botmasters to increase the size of their botnets. In this method, webpages host content that installs malicious code on visitors computers permitting botmasters to gain control. As identified by WebSense (2008),

- 75 percent of websites with malicious code are legitimate sites that have been compromised. This represents an almost 50 percent increase over the previous six-month period.
- 60 percent of the top 100 most popular web sites have either hosted or been involved in malicious activity in the first half of 2008.
- 12 percent of web sites infected with malicious code were created using Web malware exploitation kits, a decrease of 33 percent since December 2007. Websense researches believe this decrease may be attributed to attackers launching more customized attacks to avoid signature detection by security measure.
- 29 percent of malicious web attacks include data-stealing code
- 46 percent of data-stealing attacks are conducted over the web.

These figures show a potential change in threat climate pointing to internet web browsing as being a significant contributor to botnet propagation.

Lastly, botnets can exploit vulnerabilities in other malware already running on the host. For example, the Bagel and MyDoom worms contained backdoors that were exploited by botnets in April of 2004 (Cooke, Jahanian, & McPherson, 2005).

Topology based on Command and Control method

IRC botnets. The first topology seen within botnets relied heavily on Internet Relay Chat for command and control. As the birthplace of botnets, IRC channels were used for running games, file distribution, and for user misbehavior. "Early bots were not always malicious" (Bu, Bueno, Kashyap, & Wosotowsky, 2010). In IRC botnets, the IRC channel acted as the command and control server for the compromised zombies. IRC traffic typically occurred over a particular port number from zombie client to IRC server (Bailey, Cooke, Jahanian, Xu, & Karir, 2009).

Peer-to-Peer botnets

The next topology seen within botnets relies on peer-to-peer (P2P) communication for command and control. Instead of using a centralized architecture as seen in IRC botnets, P2P botnets allowed peers to connect to other peers as long as their IP address is known within the botnet database. The botmaster can inject commands to any peer within the botnet and the command is then relayed to other peers (Bailey, Cooke, Jahanian, Xu, & Karir, 2009). This type of botnet has many variations and has evolved to keep up with security researcher's attempts to track down known peers. "In the last several years, botnets such as Slapper, Sinit, Phatbot, and Nugache have implemented different kinds of P2P control architectures" (Wang, Sparks, & Zou, 2010). Some have implemented cryptography for update identification and encrypted or obfuscated control channels. Although the botmasters have evolved the malware to defeat inherent weaknesses in P2P botnets, these modifications often open up new methods for detecting and compromising the botnet's anonymity (Wang, Sparks, & Zou, 2010).

HTTP Botnets. In this topology, botnets use standard web requests that operate over port 80 to facilitate command and control. This topology uses a webserver as the centralized command and control channel similar to how IRC botnets used IRC channels. However, the web server C&C channel stays always connected with eliminates the fundamental problem of connection loss to IRC channels. In HTTP botnets, the traffic flows with regular web browsing traffic. However, the HTTP botnet traffic is structured different than normal traffic making it easier to detect (Bailey, Cooke, Jahanian, Xu, & Karir, 2009).

One of the most popular HTTP botnets found in the wild today is the ZeuS botnet. ZeuS consists of both a client and a server component where anyone with little computer expertise can create a custom version of the malware. Ironically, the current version of ZeuS uses a strict commercial software license which links directly to the buyer's physical hardware. "The creation and distribution channel of this malware displays a strong business sensibility" (Bu, Bueno, Kashyap, & Wosotowsky, 2010).

Web 2.0 Botnets. The last topology discussed is the newest growing for botnets. These botnets leverage Web 2.0 technologies often seen within social networking websites. Similar to HTTP botnets, Web 2.0 botnets utilize web applications such as Facebook, MySpace, RSS, and Blogging for command and control purposes. Although the concept of social network C&C dates back in academic work as early as 2007, the first reported botnet – named Naz – was found on Twitter.com and Jaiku.com (Kartaltepe, Morales, Xu, & Sandhu, 2010). The Naz command and control attack flow and control flow is diagramed in figure 1 below. This type of botnet exhibits the increased complexity and innovativeness of botmasters.

Intended Targets

In research conducted by Damballa (Ollmann, 2009), a distinguishing factor identified directly relates to what type of victim is targeted by a botnet: broad-spectrum internet user or the enterprise asset. In this research, 50 percent of botnets identified in the enterprise environment were *Internet Targeted* botnets. These broad-spectrum attacks are aimed at any Internet user but often enter enterprise environments due to relaxed security or usage of personally owned computing equipment in the workplace. These botnets often have readily available fixes but require enterprise security teams to patch software properly and keep anti-virus signatures up to date (Ollmann, 2009).

The next target group identified is called the *Enterprise Targeted* botnets. In this case, botnets found within the enterprise are hardly ever found circulating the Internet. These botnets are designed to penetrate and propagate within enterprise networks and are a blend of sophisticated remote access Trojans with worm propagation functions. These botnets are often targeted at specific industries such as online retail companies or specific people within the organization such as the Chief Financial Officer. These botnets are typically more advanced than *Internet Targeted* botnets. Around 35 percent of botnets encountered within the enterprise are of this type (Ollmann, 2009).

The next group identified is called the *Deep Knowledge* botnet. Although only making up 10 percent of the botnets identified in the enterprise, these botnets can be very sophisticated and very dangerous. The botmaster often has a high degree of knowledge about the infiltrated enterprise and the information architecture. It is believed that many of the *Deep Knowledge* botnets are created and installed by hand for legitimate remote administration by employees.

The bigger problem is that many commercial do-it-yourself malware construction kits have backdoors to their creators or partners (Ollmann, 2009).

That last group identified by Damballa is a catch-all group referred to as *Others.* In this group, the remaining 5 percent of botnets encountered in the enterprise vary in sophistication and functionality and don't fit neatly into any other group. These include small botnets targeted at a specific group for industrial espionage and competitive advantage or possibly state-sponsored botnets aimed at specific goals (Ollmann, 2009).

Use of Botnets

Because of the flexible nature of botnets, the use by cyber criminals is vast and evolving. One common use of botnets is the execution of Distribute Denial of Service (DDoS) attacks. In a DDoS, botnets are used to deplete the network bandwidth and other computational resources of target sits. Using a botnet for this type of attack magnifies the impact of the attack and eliminates the need to mask or spoofidentifying information (Choo, 2007). In the enterprise environment, botnet DDoS attacks may pose a substantial risk particularly for e-commerce lines of business. Also, DDoS attacks aimed at unique network resources such as the Dynamic Name Service (DNS) may prevent normal business operations within the enterprise environment. Similarly, 'spidering' attacks on a company's website uses HTTP floods that recursively access resources causing denial of service conditions (Uses of botnets, 2008)

In addition to DDoS attacks, botnets are also used for spam dissemination. In April of 2005, Symantec spam statistical report indicated that 61 percent of global email was identified as spam (Choo, 2007). The financial gain achieved by botmasters through spamming encourages ever increasing vigilance. A spambot malware, known as SpamThru, included sophisticated features that used advanced encryption, installs its own antivirus scanner to eliminate competing

malware, and even enacted functions to evade anti-spam measures (Choo, 2007). Enterprises inflicted with botnet malware may be producing spam inside the enterprise.

Information theft is a major concern for botnets in the enterprise environment as well as individual privacy for home users. Sniffing traffic and key-logging components are often found in botnet malware allowing botmasters to collect unencrypted traffic passing through the bot or log all keystrokes entered by a user (Uses of botnets, 2008). In the enterprise environment, there is a substantial risk of compromising critical sensitive information or business trade secrets. This information must then by exfiltrated back to botmasters through covert channels.

Botnets have also been used to spread new malware. Newly created malware can obtain a substantial rapid existence by using computers under the control of a botmaster to launch the new malware. Many botnets include functionality to remotely download new files and execute them. The Witty worm was initially launched through the use of an existing botnet (Uses of botnets, 2008). Botnets existing in an enterprise environment pose a substantial risk as newly released malware may not have antivirus signatures available magnifying potential compromise.

Another substantial motivator for botnet use is for financial gain. Often referred to as "click fraud", botnets are able to abuse ad programs like Google AdSense by using bots to 'click' on ads to artificially increase the click counter. The use of this type of financial gain is not common (Uses of botnets, 2008); however, a 2010 study indicated a growth in this activity with 42.6 percent of all click fraud originating from botnets (Singer, 2010). A similar type of financial gain was seen with a recent Twitter-based botnet that mines the online currency known as bitcoins. This type of botnet was aimed at stealing virtual currency by leveraging the massive distributed computing power of the botnet to solve complex mathematical tasks. Based off the bitcoin economy, the more computations a user accomplishes the more virtual currency can be

created. That virtual currency has exchange rates for conventional currency (The H Security, 2011).

Of greater concern than bitcoin mining, botnets can be used for mass identity theft. Botnets can deploy phishing scams that lure victims into entering sensitive private information into compromised or bogus websites like PayPal or banking institutions (Uses of botnets, 2008). This tactic combined with packet sniffing and key logging introduces substantial risk to the enterprise and the organization's employees.

History of botnets

The origins of botnets can be traced as far back as 1999 with the creation of the malware Sub7 and Pretty Park. Both of these offered a control method utilizing an IRC channel where the creator could send malicious commands to infected computers. A year later, the Global Threat bot, or GBOT for short, was introduced that included higher sophistication. Namely, the GBOT was able to access raw network level sockets (both connection-oriented TCP and connection-less UDP) allowing for Denial of Service attacks. Additionally, the GBOT had the ability to hijack Sub7 infected computers and "update" them to GTBots (Ferguson, The history of the botnet - Part I, 2010).

In 2002, the release of SDBot and Agobot fueled the growth of botnets and initiated the creation of variants. These two botnets introduced techniques such as creating backdoors, disabling anti-virus, and blocking access to security vendor websites. These early botnets were aimed at information theft and remote control. SDBot, due to the public release of its source code, became the standard for several variants including the Spybot botnet in 2003. With Spybot came new functionality such as key logging, data mining, and Instant Messaging Spam (SPIM) (Ferguson, The history of the botnet - Part I, 2010).

Also in 2003, two more significant functionalities were first seen in the wild. First, the Rbot botnet introduced proxying for relaying commands and the coordinated Distributed Denial of Service (DDoS) attack. Rbot also included information stealing tools as well as encryption techniques to try to evade detection. Second, the Sinit botnet introduced a new topology of peer-to-peer. This marked the evolution of botnets away from the IRC command and control channels due to easy detection and frequent blocking at enterprise boundary firewalls (Ferguson, The history of the botnet - Part I, 2010).

Criminal interests surfaced in 2003 with several botnets that facilitated spamming. The Beagle, Bobax, and Mytob botnets included mass-mailing functionalities enabling criminals to distribute their spam with agility, flexibility, and covertly to avoid ever increasing law enforcement efforts (Ferguson, The history of the botnet - Part II, 2010).

Throughout the next several years, many famous botnets were introduced. RuStock in 2006 and the infamous ZeuS crimeware family. As an information stealing tool, ZeuS has been updated to newer versions several times with increased functionality and lethality. The botnet interfaces have been designed to entice less technically savvy criminals by allowing for simple point and click controls. Subsequently, developers have included backdoors in the command and control software turning criminal controllers of botnets into victims as well (Ferguson, The history of the botnet - Part II, 2010).

Efforts to fight back have been launched by government and private companies. In 2008, two Internet Service Providers de-peered – or stopped routing traffic – the McColo hosting provider which routinely hosted command and control servers for botnets. This takedown resulted in a 75% reduction in spam Internet-wide (Security Focus, 2008). In June of 2009, the Federal Trade Commission closed down the Internet Service Provider ‘3FN’ which impacted

some botnet command and control networks. Despite efforts to disrupt these botnets, the creators become more innovate and increase efforts at evading detection. One technique used by the Conflicker botnet was to generate 50,000 alternative hostnames daily making in near impossible for the security industry to block them all (Ferguson, The history of the botnet - Part II, 2010).

In the late 2007s, the landscape of botnets continued to evolve into the Web 2.0 technologies. Having left behind IRC and basic peer-to-peer command and control, alternate channels were embedded in blogs and Real Simple Syndication (RSS) feeds. Criminal innovation continues to evolve as seen by ZeuS bot storing configuration files in the compromised Amazon EC2 cloud service. With botmasters using Facebook, Twitter, and Google as command and control channels, detection has become more and more difficult as communication to these sites is very common and expected. Finding the hidden, covert channels is and will continue to be challenge for security specialists. Future expectations include use of highly effective encryption techniques such as Public Key Infrastructure (PKI) and advanced peer-to-peer cloud services. Already in use, the Koobface botnet uses social networking services for propagation of spam by sending messages, making posts, and even creating it's own Facebook profile page (Ferguson, The history of the botnet - Part III, 2010) (Ferguson, 2010 - Year of the Zombie Cloud?, 2010).

Part II – The Mitigation

This section of the paper proposes an approach to mitigating the threat of botnets to the enterprise environment. In this part, the term 'organization' is used to describe any enterprise environment including government, corporate, or non-profit sector. The proposed approach to mitigating botnet risks involves usage of the Enterprise Architecture framework developed by Dr. Scott Bernard (Bernard S. A., 2005) and the Information Technology Security Architecture (Bernard & Ho, 2008). A list of 19 botnet related risks has been developed by reviewing the literature included in Part I of this paper and can be found in table 1. Part II will apply the ITSA framework found within EA and offer mitigation recommendations in context.

Enterprise Architecture and the Information Technology Security Architecture Overview

Enterprise Architecture is the "analysis and documentation of an enterprise in its current and future states from an integrated strategy, business, and technology perspective" (Bernard S. A., 2005, p. 31). EA, as a management program, enables organizations to have a holistic view from top-level strategy down to the lowest level of technology infrastructure. These vertical components of the framework help organizations understand the ties between strategy, information, and technology. Additionally, the EA framework introduces threads which define common activities always present across all levels of the framework: namely security, standards, and workforce considerations. In addition to being a management program, the EA is also a documentation program that provides a methodology for developing current and future views of the enterprise (Bernard S. A., 2005).

Within the EA^3 cube, another integrated framework exists that provides confidentiality, integrity, and availability of information throughout the enterprise. The Information Technology Security Architecture (ITSA) defines corresponding layers: (1) information security governance; (2) operations security; (3) personnel security; (4) information and data flow security; (5) systems security; and (6) application development security; (7) infrastructure security; and (8) physical security (Bernard S. , 2008-2009). The ITSA works in the context of EA by relating security concepts and goals to the corresponding EA^3 Framework level (Bernard & Ho, 2008).

Mitigating Factors – Information Security Governance

According to Bernard & Ho (2008), this layer of the ITSA is to "define security strategies, policies, standards and guidelines for the enterprise from an organizational viewpoint" (p. 11). The activities associated with this layer include both procedural and documentation

functions. Traditionally, this layer includes high level policy statements, access definition policies, fair information practices, and security lifecycle charts (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA directs the high level strategic approach. Success at this layer requires well rounded procedures and policies aimed at protecting the enterprise environment through defense in depth. In table 2, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the information security governance layer of the ITSA.

Generally speaking, drafting security policies should focus on the principles needed to meet the required compliance level. This ensures that there is a required need for such a policy and that it aligns with the mission statement. Other concerns to keep in mind and avoid are contradictions with other policies, unintended loopholes, excessive cost in terms of time and resources, and over complicated wording (Bernard & Ho, 2008).

Mitigating Factors – Operations Security

According to Bernard & Ho (2008), this layer of the ITSA is to "define the enterprise's intra-organizational and operational needs as they interact with and require access to the enterprise IT services, in order to identify and address security needs at the enterprises organizational level" (p. 12). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes risk assessments, authorization models, access control user requirements, business impact analysis, disaster recovery and business resumption planning (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA addresses risk management and continuity of operations. In table 3, the following list of botnet security

concerns from table 1 represents a list of some risk areas that can be partially mitigated within operations security layer of the ITSA.

Mitigating Factors – Personnel Security

According to Bernard & Ho (2008), this layer of the ITSA is to "ensure that enterprise personnel are accessing and utilizing its information and technology services safely, securely, and in accordance with their predefined roles and responsibilities of their job functions, through proper access control plans and detection of employee anomalous behavior" (p. 15). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes user authentication, role-based access control, awareness training, desktop security policies, and procedural training (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA is important for setting expectations of employee behavior and responsibility for information security practices. This layer will emphasize personnel security threats in relation to botnet risk areas. Additionally, this layer establishes an information security training process which can contribute to reducing risk introduced by the human element. In table 4, the following list of botnet security concerns from table 1 represents a list of risk area topics that can be partially mitigated within the personnel security layer of the ITSA.

Mitigating Factors – Information and Data Flow Security

According to Bernard & Ho (2008), this layer of the ITSA is to "identify and classify information and data as it moves through the enterprise – in order to justify adequate security controls" (p. 16). Within this layer, information needs to be valued and classified into levels depending on risk. Traditionally, this layer includes data design, dataflow assurance, information

classification forms, logical access controls, and associative access controls (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA indirectly affects several risk area topics. Information classification is a necessity for identifying appropriate levels of protection. In table 5, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the information and data flow security layer of the ITSA.

Mitigating Factors – Systems Security

According to Bernard & Ho (2008), this layer of the ITSA is to "protect sensitive applications and provide granularity of access controls to sensitive resources" (p. 20). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes user account management, certificate request management, password storage and management, remote access, authorization models, file system hardening procedures, patching, and security repositories (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA protects systems and operating systems through the use of host intrusion detection, authentication and authorization models, and public key infrastructure. In table 6, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the systems security layer of the ITSA.

Mitigating Factors – Application Development Security

According to Bernard & Ho (2008), this layer of the ITSA is to "design authentication, authorization and accounting (AAA) components into the applications used in the enterprise; to enforce the application process flow throughout the enterprise; and to ingrain security in the

[Software Development Life Cycle] SDLC" (p. 18). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes design and development, application development security, application gateways, and application security placement (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA can minimize in-house developed software application vulnerabilities with potential for botnet exploitation. In table 7, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the application development security layer of the ITSA.

Mitigating Factors – Infrastructure Security

According to Bernard & Ho (2008), this layer of the ITSA is to "develop a secure infrastructure that meets all security requirements of the enterprise and can safeguard against future attacks against the enterprise" (p. 22). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes network partitioning, VLANs, firewalls, packet filtering, circuit level gateways, PKI architectures, VPNs, SSL, and stateful inspections (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA is where the figurative rubber meets the road. In table 8, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the infrastructure security layer of the ITSA.

Mitigating Factors – Physical Security

According to Bernard & Ho (2008), this layer of the ITSA is to "construct a perimeter physical defense system that safeguards the facility and physical resources for the enterprise" (p.

25). The activities associated with this layer include both procedural and documentation functions. Traditionally, this layer includes building and facility security, physical access controls, network operation centers server rooms, wiring closets, and cable plants (Bernard & Ho, 2008).

In relation to protection for botnet-related risks, this layer of the ITSA can reduce the risk of botnet propagation. In table 9, the following list of botnet security concerns from table 1 represents a list of some risk areas that can be partially mitigated within the physical security layer of the ITSA.

Part III – Case Study: Georgia

During the month of August 2008, the Republic of Georgia imposed a state of war against Russia due to military actions that crossed the demilitarized zone of South Ossetia (Tikk, Kaska, Runnimeri, Kert, Taliharm, & Vihul, 2008). Although a physical war followed, the preceding cyber war is of particular interest. This short case study will review the steps taken by Russian hackers to launch a pre-emptive strike against Georgia and will review the actions taken by Georgia to mitigate those cyber attacks.

During the cyber attacks, several methods were used to degrade Georgia's internal communication and with their ability to update the international community on war efforts. This was accomplished in several ways: by defacing government websites and coordinating Denial of Service attacks and/or Distributed Denial of Service attacks. First, the defacement of Georgian websites was used as psychological warfare by publishing images correlating the current President with other 20th century dictators. This was accomplished by Russian threat actors distributing a listing of known SQL injection vulnerabilities along with exploit tools in public

forums encouraging anti-Georgian hackers to take action (Tikk, Kaska, Runnimeri, Kert, Taliharm, & Vihul, 2008).

Second, Denial of Service attacks were launched against private and public sector websites including news and banking websites. These attacks were highly coordinated with average traffic data reaching 211.66 Mbps and maximum traffic data peaking at 814.33Mbps. "The major DDoS attacks observed were all globally sourced, suggesting a botnet (or multiple botnets) behind them" (Tikk, Kaska, Runnimeri, Kert, Taliharm, & Vihul, 2008, p. 12). The Shadowserver Foundation identified at least six different command and control servers involved in the attack, including DDoS for hire and DDoS for extortion services. One botnet identified was a tool often used by Russian botmasters with seemingly bogus domain registration data. Furthermore, some research indicates potential involvement of the Russian Business Network (RBN) cyber criminal syndicate; however, it is believed that the RBN did not directly carry out the attacks (Tikk, Kaska, Runnimeri, Kert, Taliharm, & Vihul, 2008).

In response to these cyber attacks, the Republic of Georgia implemented a simple yet highly effective countermeasure. First, some of the websites being attacked changed their Internet Protocol (IP) address in efforts to thwart the attacks while others changed their hostnames. Second, several of the news outlets moved services to blogspot.com and other blogging public websites. Most notably, the Georgia Ministry of Defense and the President completely relocated their websites to Tulip Systems, Inc., located in Atlanta, Georgia, USA. The Ministry of Foreign Affairs also moved their website to an Estonian server to avoid the denial of service attacks (Tikk, Kaska, Runnimeri, Kert, Taliharm, & Vihul, 2008).

The 'maneuver' Georgian response to Distributed Denial of Service attacks offers a relatively simple solution that fits nicely into the Information Technology Security Architecture.

Through use of holistic planning, organizations can accomplish similar end results seen by Georgia through effective governance and successful business continuity planning. Botnet threat activity in the form of Distributed Denial of Service attacks can disable an organization's ability to conduct business processes. Having alternative routes and redundant sites (such as hot or warm sites) can provide an option for organizations to essentially move out of the way during an attack. It is unknown whether Georgia's reactions to cyber attacks were pre-planned or not; however, this relatively small country was able to show resilience to information warfare. Most importantly, this case study gives a real life example of how a holistic approach to information security and botnet defense – including business continuity planning – can help reduce the impact of cyber attack.

Part IV – Conclusion

In conclusion, botnet activity is a substantial threat to the enterprise environment. With evolving capabilities, botmasters will continue to stay at the cutting edge of technology and devise new ways to avoid detection. Part I of this paper discussed the evolution of botnets from the days of Internet Relay Chat to the modern social media. Propagation techniques have evolved to stay ahead of security professionals and some advanced botnets are specifically designed to attack an intended target of the enterprise environment. Lastly, part I briefly described some of the malicious activities that botmasters use botnets for including distributed denial of service and for-profit activities. Throughout part I, 19 risk area topics were identified that directly relates to botnet activity. If unmitigated, these risk area topics can result in botnet infection and subsequent damages.

Part II of this paper introduced a method to mitigate the risk area topics by implementing the Enterprise Architecture and Information Technology Security Architecture models. Through the layers of these models, it was shown that many of the botnet risks can be mitigated by implementing a holistic approach to information security.

Lastly, Part III of this paper provided a case study where a nation-state uses part of the business continuity planning process of the Information Technology Security Architecture to mitigate a distributed denial of service attack.

References

(IN)Secure. (2010, April 02). *Botnets drive the rise of ransomeware*. Retrieved April 25, 2012, from Help Net Security: http://www.net-security.org/secworld.php?id=9095

Uses of botnets. (2008, August 10). Retrieved April 22, 2012, from The Honeynet Project: http://www.honeynet.org/node/52

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009). *A Survey of Botnet Technology and Defenses.* Ann Arbor, MI.

Bernard, S. (2008-2009). *Enterprise Information Security Architecture V2.2.* KSA Learning Point 5.7.

Bernard, S. A. (2005). *An Introduction to Enterprise Architecture: second edition.* Bloomington, IN: AuthorHouse.

Bernard, S., & Ho, S. M. (2008). Enterprise Architecture as Context and Method for Designing and Implementing Information Security and Data Privacy Controls in Government Agencies.

Bu, Z., Bueno, P., Kashyap, R., & Wosotowsky, A. (2010). *The New Era of Botnets.* Santa Clara, CA: McAfee Labs.

Choo, K.-K. R. (2007). *Zombies and botnets.* Woden: Australian Institute of Criminology.

Cooke, E., Jahanian, F., & McPherson, D. (2005). *The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets.* Ann Arbor, MI: University of Michigan and Arbor Networks.

Dagon, D. (2005). *Botnet Detection and Response: The Network is the Infection.* Retrieved Aorik 22, 2012, from OARC Workshop: http://www.caida.org/funding/dns-itr/events/200507/slides/oarc0507-Dagon.pdf

Dagon, D., Gu, G., Lee, C. P., & Lee, W. (n.d.). *A Taxonomy of Botnet Structures.* Atlanta, GA: Georgia Institute of Technology.

Damballa. (2011, February 8th). *Canned Sandboxing*. Retrieved April 26, 2012, from Damballa - The Day Before Zero: http://blog.damballa.com/?p=1097

Ferguson, R. (2010, December 15). *2010 - Year of the Zombie Cloud?* Retrieved April 20, 2012, from TrendMicro - ConterMeasures Blog: http://countermeasures.trendmicro.eu/2010-year-of-the-zombie-cloud/

Ferguson, R. (2010, September 24). *The history of the botnet - Part I*. Retrieved April 19, 2012, from TrendMicro - CounterMeasures Blog: http://countermeasures.trendmicro.eu/the-history-of-the-botnet-part-i/

Ferguson, R. (2010, September 27). *The history of the botnet - Part II*. Retrieved April 19, 2012, from TrendMicro - CounterMeasures Blog: http://countermeasures.trendmicro.eu/the-history-of-the-botnet-part-ii/

Ferguson, R. (2010, November 5). *The history of the botnet - Part III*. Retrieved April 19, 2012, from TrendMicro - CounterMeasures Blog: http://countermeasures.trendmicro.eu/the-history-of-the-botnet-part-iii/

Haag, S., Cummings, M., & Rea, Jr, A. I. (2004). *Computing Concepts, 2nd Edition.* McGraw-Hill Higher Education.

Hinson, G. (2008, April 29). *CERT's podcasts: Security for Business Leaders: Show Notes*. Retrieved April 25, 2012, from Cert.org: http://www.cert.org/podcast/notes/20080429hinson-notes.html

Kartaltepe, E. J., Morales, J. A., Xu, S., & Sandhu, R. (2010). *Social Network-Based Command-and-Control: Emerging Threats and Countermeasures.* San Antonio, TX: Springer-Verlag Berlin Heidelberg.

Kolakowski, N. (2010, March 03). *Spain, IT Security Companies Sting Mariposa Botnet.* Retrieved April 22, 2012, from eWeek: IT Security & Network Security News: http://www.eweek.com/c/a/Security/Spain-IT-Security-Companies-Sting-Mariposa-Botnet-390027/

Martin, R. A. (2003). Integrating Your Information Security Vulnerability Management Capabilities Through Industry Standards (CVE & OVAL). *IEEE*, 1528-1533.

McAfee, Inc. (n.d.). *Network Intrusion Prevention*. Retrieved April 26, 2012, from McAfee.com: http://www.mcafee.com/us/products/network-security/network-intrusion-prevention.aspx

MXPolice. (2011, July 1). *Zeus Botnet Being Spread Through Fake IRS Spam Campaign.* Retrieved April 22, 2012, from MXPolice.com: http://www.mxpolice.com/spam-trends/zeus-botnet-being-spread-through-fake-irs-spam-campaign/

Nagaraja, S., Houmansadr, A., Piyawongwisal, P., Singh, V., Agarwal, P., & Borisov, N. (n.d.). *Stegobot: a covert social network botnet.* New Delhi, India & Urbana, IL.

Naseem, F., Shafqat, M., Sabir, U., & Shahzad, A. (2010). A Survey of Botnet Technology and Detection. *International Journal of Video & Image Processing and Network Security*, 13-17.

Ollmann, G. (2009, November 25). *Enterprise versus Broad-spectrum Internet Botnets*. Retrieved April 19, 2012, from Damballa Blog: The Day Before Zero: http://blog.damballa.com/?p=426

Raywood, D. (2010, November 29). *A condensed history of the botnet*. Retrieved April 19, 2012, from SCMagazine UK: http://www.scmagazineuk.com/a-condensed-history-of-the-botnet/article/191636/

Scambusters. (2006). *Ransomware: How to Protect Yourself*. Retrieved April 25, 2012, from Scambusters.org: http://www.scambusters.org/ransomware.html

Schectman, J. (2012, April 12). *Get Ready for the Return of the Botnets*. Retrieved April 29, 2012, from wsj.com: http://mobile.blogs.wsj.com/cio/2012/04/12/get-ready-for-the-return-of-the-botnets/

Security Focus. (2008, November 13). *McColo takedown nets massive drop in spam*. Retrieved April 20, 2012, from Security Focus: http://www.securityfocus.com/brief/855

Singer, M. (2010). *Security and the Virtual Enterprise.* Retrieved April 26, 2012, from AT&T: http://www.corp.att.com/tlf/docs/singer_presentation.pdf

The H Security. (2011, August 25). *Botnet attacks pizza delivery service*. Retrieved April 19, 2012, from The H Security: http://www.h-online.com/security/news/item/Botnet-attacks-pizza-delivery-service-1330816.html

The H Security. (2011, April 4). *Twitter-controlled botnet mines Bitcoins*. Retrieved April 19, 2012, from The H Security: http://www.h-online.com/security/news/item/Twitter-controlled-botnet-mines-Bitcoins-1318497.html

Tikk, E., Kaska, K., Runnimeri, K., Kert, M., Taliharm, A.-M., & Vihul, L. (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified.* Tallinn, Estonia: CCDCOE.

Wang, P., Sparks, S., & Zou, C. C. (2010). An Advanced Hybrid Peer-to-Peer Botnet. *IEEE Transactions on Dependable and Secure Computing, Vol. 7*(No. 2), 113-127.

Websense. (2008). *Websense Security Labs: State of Internet Security Q1-Q2, 2008.* Websense, Inc.

Xin-liang, W., Lu-Ying, C., Fang, L., & Zhen-ming, L. (2010). *Analysis and Modeling of the Botnet Propagation Characteristics.* Beijing, China: IEEE- Beijing University of Posts and Telecommunications.

Zavoina, A. (1998). Crafting an Internet Acceptable Use Policy. *ABA Bank Compliance*, 29-31.

Zhang, G.-Y., Li, J., & Gu, G.-C. (2004). Research on Defending DDoS Attack - An Expert System Approach. *2004 IEEE International Conference on Systems, Man and Cybernetics*, 3554-3558.

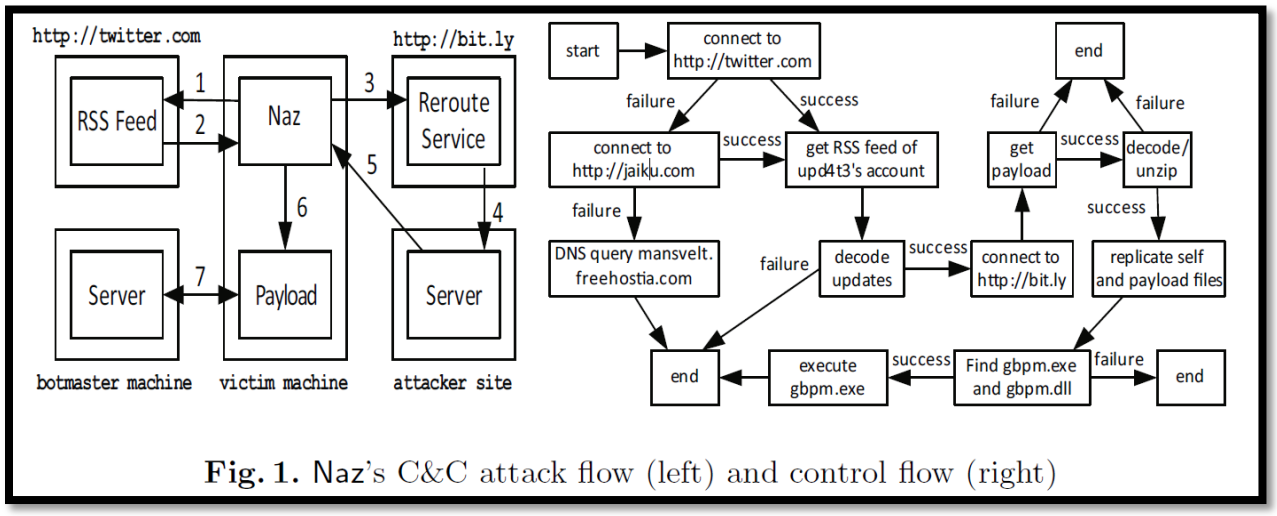

Fig. 1. Naz's C&C attack flow (left) and control flow (right)

Figure 1: Command and Control attack flow utilizing Web2.0 technologies. Twitter.com along with RSS feeds (Kartaltepe, Morales, Xu, & Sandhu, 2010).

Table 1

Botnet Risk topics cross-referenced with ITSA layers.

	Corresponding ITSA layer							
Botnet Risk Area Topics	IS Governance	Operations Security	Personnel Security	App Development	Info & Data Flow	Systems Security	Physical Security	Infrastructure Security
Data exfiltration (information theft) through file system infiltration	*X*	*X*			*X*	*X*	*X*	*X*
Packet Sniffing	*X*	*X*			*X*	*X*		*X*
Key logging	*X*	*X*			*X*	*X*		*X*
Distributed Denial of Service	*X*	*X*			*X*	*X*		*X*
Spamming	*X*				*X*	*X*		*X*
Zero-day malware distribution	*X*	*X*		*X*	*X*			
Click Fraud for profit								*X*
Extortion and blackmail (Ransomware)	*X*		*X*		*X*	*X*		*X*
Remote Control	*X*	*X*			*X*	*X*		*X*
Disabling of AntiVirus	*X*	*X*			*X*	*X*		*X*
Blocking access to Security Vendor websites	*X*	*X*			*X*	*X*		*X*
Original programmer backdoors	*X*			*X*	*X*			*X*
Web browsing to malicious websites (even legitimate websites that have been exploited)	*X*	*X*	*X*		*X*	*X*		*X*
Relaxed Security processes	*X*		*X*		*X*	*X*		
Use of personal equipment in workplace	*X*		*X*		*X*		*X*	*X*
Social engineering attacks on instant messaging programs	*X*		*X*		*X*			*X*
Social engineering attacks in malicious email	*X*		*X*		*X*	*X*		*X*
Vulnerabilities in operating systems	*X*	*X*			*X*	*X*		*X*
Vulnerabilities in Applications	*X*	*X*		*X*	*X*			*X*

Table 2

Botnet Risk Area topics and corresponding governance mitigation.

Risk Area Topics	Governance Mitigation
1. Data exfiltration (information theft) through file system infiltration 2. Packet Sniffing 3. Key Logging 4. Disabling of AntiVirus 5. Original programmer backdoors 6. Vulnerabilities in operating systems 7. Vulnerabilities in applications 8. Relaxed Security processes 9. Blocking access to Security Vendor websites 10. Zero-day malware distribution 11. Remote Control 12. Spamming 13. Distributed Denial of Service	These risk areas can be mitigated through usage of standards defined by Bernard & Ho (2008) as "a set of rules and regulations that control how information systems, materials, products, services, technologies, and management processes, etc. should be developed, managed and operated" (p. 12). Since most of these risks are technical in nature with corresponding layers lower in the ITSA, governance can help define the guidelines, policies, and baselines to govern systems, service, applications and the technology on which they reside (Bernard & Ho, 2008). Adopting industry best practices and proven standards at the top level of the ITSA results in higher organizational maturity and a better security posture. For example, an organization may reduce the risk of botnet propagation by adopting standards related to vulnerability management. In particular, the Common Vulnerability and Exposures Initiative (CVE) and Open Vulnerability Assessment Language (OVAL) initiative defines conventions to make organizing information related to security vulnerabilities "less of a labor intensive art and more of an engineer practice" (Martin, 2003).

14. Social engineering attacks on instant messaging programs 15. Social engineering attacks in malicious email 16. Use of personal equipment in workplace 17. Web browsing to malicious websites (even legitimate websites that have been exploited) 18. Extortion and blackmail (Ransomware)	This risk area can be mitigated through strong policy governing user actions and appropriate usage agreements. Having users agree to and sign acceptable use policies may result in reduced risk of virus and other malicious activity (Zavoina, 1998). The key to mitigating botnet risks in these risk areas is development and compliance with policy aimed to keep users away from potential malicious websites and learn the best responses to social engineering attempts. These policies link back to the organization's strategic goals and affect many other subordinate ITSA layers.

Table 3

Botnet Risk Area topics and corresponding Operations Security mitigation.

Risk Area Topics	Operations Security Mitigation
1. Data exfiltration (information theft) through file system infiltration 2. Packet Sniffing 3. Key logging 4. Zero-day malware distribution 5. Disabling of AntiVirus 6. Remote Control 7. Web browsing to malicious websites 8. Blocking access to Security Vendor websites	As discussed in Bernard & Ho (2008), one focus of the Operations Security layer is on the Incident Handling Team's ability to resolve security incidents by amending vulnerabilities, quarantining malicious codes and viruses, restoring infected information systems, and to prevent future damages (p. 14). The impact of each of these risk area topics can be reduced by successful usage of an incident handling team. For example, the impact of blocked access to security vendor websites can be reduced if proper handing occurs of outdated antivirus notifications. By properly handling this type of incident, the incident handling team can identify associated botnet malware and take remediation attempts ultimately reducing overall botnet risk. Additionally, Bernard & Ho (2008) advocate creation of a Security Operations Center (SOC) within the Operations Security Layer of the ITSA (p. 14). Within the SOC, the organization further reduces impact of these risk area topics by assigning responsibility to an organization for centralized management of the incident response processes.

9. Vulnerabilities in operating systems 10. Vulnerabilities in Applications	As discussed in Bernard & Ho (2008), another focus of the Operations Security Layer is on vulnerability assessment. By conducting self-assessments across the four phases - Discovery, Manual Inspection, Vulnerability Testing, and Process Validation - (p. 13), organizations may reduce the overall number of vulnerabilities in operating systems and application impacting the ability for a botnet to propagate.
11. Distributed Denial of Service	As discussed in Bernard & Ho (2008), another focus of the Operations Security Layer is on contingency planning and disaster recovery planning. A contingency refers to "incidents that may disrupt systems or business operations. Contingency planning means that [the] business has [an] immediate incident handling/response plan at both management as well as technical support level" (Bernard & Ho, 2008, p. 13). Because a botnet initiated distribute denial of service attack will disrupt systems and business operations, this layer of the ITSA can help mitigate that risk by defining actions to take during a DDoS attack. See *Part IV – Case Study* for an example of a botnet initiated DDoS attack subverted through use of a continuity plan.

Table 4

Botnet Risk Area topics and corresponding Personnel Security mitigation

	Risk Area Topics	**Personnel Security Mitigation**
1.	Extortion and blackmail (Ransomware)	As discussed in Bernard & Ho (2008), the personnel security layer of the ITSA is concerned with threats in personnel security, specifically physical threat from terrorists by kidnaping or extortion (p. 15). Although not to the same level of severity, botnet activity by the Bredolab and Pushdo botnets has been tied to extortion of money from victims ((IN)Secure, 2010). Ransomware techniques vary. One technique convinces the user into downloading and installing malware by tricking her into thinking she has already been infected and her download will fix the problem. Other ransomware malware blatantly disables systems until the user pays money to the attacker (Scambusters, 2006). Either way, ransomware is a form of extortion which can be mitigated through the personnel security layer of the ITSA.
2.	Web browsing to malicious websites (even legitimate websites that have been exploited)	As discussed in Bernard & Ho (2008), another important aspect of the personnel security layer of the ITSA is annual security awareness training for all employees (p. 16). This includes the signing of security awareness agreements that explicitly state that monitoring and auditing of employee and administrator
3.	Relaxed Security processes	
4.	Use of personal equipment in workplace	
5.	Social engineering attacks on instant	

messaging programs 6. Social engineering attacks in malicious email	behavior is standard practice and should be expected (Bernard & Ho, 2008). To help mitigate the botnet risk areas related to social engineer attacks, specific material related to identification of attacks should be included in the organization's security training package. "Raising awareness and conducting regular training are key, given that the only truly effective control is through people" (Hinson, 2008) Educating employees on phishing and spear phishing trends and inventing innovative ways to increase employee knowledge can help reduce the possibility of occurrence of these botnet related risk area topics.

Table 5

Botnet Risk Area topics and corresponding Information and Data Flow Security mitigation

Risk Area Topics	Information and Data Flow Security Mitigation
1. Data exfiltration (information theft) through file system infiltration 2. Packet Sniffing 3. Key logging 4. Distributed Denial of Service 5. Spamming 6. Zero-day malware distribution 7. Extortion and blackmail (Ransomware) 8. Remote Control 9. Disabling of AntiVirus 10. Blocking access to Security Vendor websites 11. Original programmer backdoors 12. Web browsing to malicious websites (even legitimate websites that have been exploited) 13. Relaxed Security processes 14. Use of personal equipment in workplace 15. Social engineering attacks on instant messaging programs 16. Social engineering attacks in malicious email 17. Vulnerabilities in operating systems 18. Vulnerabilities in Applications	The information and data flow security layer of the ITSA has an indirect impact on every identified botnet risk area topic. According to Bernard & Ho (Bernard & Ho, 2008), justifying adequate levels of security controls requires classification of information and data as it moves through the enterprise (p. 16). The level of classification drives which controls are needed. For example, preventing data exfiltration of a company's trade secrets will require more security controls than protecting publicly available information from exfiltration. Furthermore, having relaxed security processes may not be important if the information being protected does not have a requirement for high levels of availability, confidentiality, and integrity. Also relevant for this layer is the role that security models play in the overall protection of information from botnets. For example, the Biba Integrity Model prevents unauthorized users from making modifications (Bernard & Ho, 2008). Based off this model, botnet activity would not have adequate permissions

	to make changes to a system which, for example, could disable anti-virus software or remote control the computer. Lastly, the process of risk management, analysis, and assigning risk controls resides in this layer of the ITSA model (Bernard & Ho, 2008). Since the overall functioning of a security program and protecting an organization's information is risk based, the ITSA can help mitigate botnet risks and protect the organization's resources. The overall risk management program oversees the analysis and assignment of risk controls to reduce vulnerabilities, prevent information exfiltration, protect from social engineering attacks, and determine remedial actions for distributed denial of service attacks. Risk management and botnet mitigation activities go hand and hand.

Table 6

Botnet Risk Area topics and corresponding Systems Security mitigation

	Risk Area Topics	Systems Security Mitigation
1.	Data exfiltration (information theft) through file system infiltration 2. Packet Sniffing 3. Key logging 4. Spamming 5. Extortion and blackmail (Ransomware) 6. Remote Control 7. Disabling of AntiVirus 8. Blocking access to Security Vendor websites 9. Original programmer backdoors	According to Bernard & Ho (Bernard & Ho, 2008), a Host-based Intrusion Detection System (HIDS) monitors incidents occurring in an information system or on a network. HIDS monitors system files, logs, logon activity, and processing with the kernel and other resources" (pg. 22). The use of a HIDS can substantially impact both botnet propagation and the ability for infected systems to communicate back to the botmaster. The HIDS can deny unexpected outbound traffic preventing data exfiltration and effectively disable command and control covert channels including original programmer backdoors.
10.	Vulnerabilities in operating systems	This layer of the ITSA addresses system hardening which is essential in the prevention of vulnerability exploitation. Hardening the system is accomplished by determining unused services and closing unnecessary ports (Bernard & Ho, 2008).
11.	Distributed Denial of Service	Authentication and Authorization information can be used to mitigate distribute denial of service attacks. By use of an Expert System model, the system uses access control information to create a filter policy during a DDoS attack (Zhang, Li, & Gu, 2004). By

	using access control lists and blacklisting, Zhang et. al. (2004) proposes that DDoS attack effectiveness can be reduced.
12. Social engineering attacks on instant messaging programs 13. Social engineering attacks in malicious email 14. Web browsing to malicious websites (even legitimate websites that have been exploited)	This layer of the ITSA also addresses Public Key Infrastructure (PKI) enabling of applications. The use of digital signatures within applications like instant messaging and email can reduce the likelihood of exploit through social engineering deception. Additionally, PKI can help prevent malicious websites from deceiving users into entering sensitive information by providing a mechanism to validate the legitimacy of the website.

Table 7

Botnet Risk Area topics and corresponding Application Development Security mitigation

Risk Area Topics	Application Development Security Mitigation
1. Original programmer backdoors	Although organization's can't directly reduce the risk of botnet programmer backdoors within this layer of the ITSA, the organization can still implement establish programming best practices preventing applications developed in house from containing backdoors. According to Haag et. al. (2004), "programmers routinely create programming backdoors when they develop software. They close most of the backdoors before releasing the program… [but] occasionally programmers forget to close all of the backdoors." Having a backdoor created during software development may increase risk of botnet exploitation.
2. Vulnerabilities in Applications	This layer of the ITSA includes best practices for development and inclusion of security throughout the software lifecycle subsequently reducing number of vulnerabilities' in applications. Furthermore, the defense-in-depth concept includes designing secure applications that understand environmental risks so that applications can be developed securely (Bernard & Ho, 2008). Less vulnerabilities means less potential exploits that a botnet can use to establish a foothold within an enterprise.
3. Zero-day malware distribution	This layer of the ITSA also can help reduce the

	impact of zero-day malware exploits in applications. By implementing sandboxing, application developers may create a safe environment for which the application relies separating it from the underlying operating system. The sandbox encases and contains the exploit attempt for unknown zero-day vulnerabilities (Damballa, 2011).

Table 8

Botnet Risk Area topics and corresponding Infrastructure Security mitigation

	Risk Area Topics	**Infrastructure Security Mitigation**
1.	Data exfiltration (information theft) through file system infiltration 2. Distributed Denial of Service 3. Spamming 4. Zero-day malware distribution 5. Click Fraud for profit 6. Extortion and blackmail (Ransomware) 7. Remote Control 8. Original programmer backdoors 9. Relaxed Security processes 10. Use of personal equipment in workplace 11. Social engineering attacks on instant messaging programs 12. Social engineering attacks in malicious email	Network Intrusion Detection Systems can be a critical tool for botnet prevention and detection. As described by Bernard & Ho (2008), the NIDS "detects probing, network configuration vulnerabilities, and monitors for attacks to and from nodes while having little impact on network traffic" (p.23). By analyzing traffic trends, a NIDS may detect data being exfiltration. NIDS can also check for signatures of known botnet malware identifying ransomware, remote control, and usage of backdoors. Some NIDS can also help detect unauthorized systems such as personal equipment as seen in the McAfee NIDS product ePolicy Orchistrator and Rogue System Detection (McAfee, Inc.).
1.	Web browsing to malicious websites (even legitimate websites that have been exploited)	Firewall Security provides perimeter security with stateful inspection of each packet deciding whether to accept, deny, or discard that packet (Bernard & Ho, 2008). The infrastructure layer of the ITSA offers mitigation of botnet risks related to malicious attacks from websites by blocking access to known malicious domains.
1.	Packet Sniffing	Lastly, network partitioning offers a defense against the sniffing risk area topic. By

	"creating logical groups and users/system to contain the flow of information, these virtual networks prevent sniffing activities because nodes are not allowed to see each other's ports without permission" (Bernard & Ho, 2008).

Table 9

Botnet Risk Area topics and corresponding Physical Security mitigation

	Risk Area Topics	Physical Security Mitigation
1.	Vulnerabilities in operating systems	As described by Bernard & Ho (2008), the physical security layer of the ITSA is an essential part of the information security architecture (p. 25). One direct way that this layer of the ITSA can reduce botnet risks is through management of removable media. As seen in the Conflicker botnet, USB removable storage is a successful propagation method (Singer, 2010). An organization that has strict physical security policy preventing usage of removable media can reduce botnet propagation risks.
2.	Use of personal equipment in workplace	At the physical layer, banning employees from using personal equipment and from allowing employees to have said equipment in their possession can reduce the likelihood of botnet propagation.

About the author

Author: Christopher Furton

Website: Http://christopher.furton.net

Certified professional with over 12 years of Information Technology experience and 8 years of hands-on leadership. An expert in cyber security with both managerial and technical skills proven throughout a career with increasing responsibility and performance expectations. Known ability to translate complex information for universal understanding. Detail-driven, results-focused leader with superior analytical, multitasking, and communication skills. Well-versed in industry best practices including Project Management and IT Service Management. Currently holding active CISSP, CEH, ITIL Foundations, Security+, and Network+ certifications.

Visit the auhor's blog:
IT Management Perspectives - https://christopherfurton.wordpress.com/

Social Sphere:

LinkedIn | Twitter | Google+ | Quora | Wordpress | Flavors.me

Slide Share | Tumblr | YouTube | Pinterest | About.me | Vimeo