Botnets as an Instrument of Warfare

Eric Koziel, David Robinson

Chapter 2

BOTNETS AS AN INSTRUMENT OF WARFARE

Eric Koziel and David Robinson

Abstract The use of botnets for malicious activities has grown significantly in recent years. Criminals leverage the flexibility and anonymity associated with botnets to harvest personal data, generate spam, distribute malware and launch distributed denial-of-service attacks. These same attributes readily translate to applications that can support operations in warfare. In 2007, distributed denial-of-service attacks launched by botnets targeted IT assets belonging to Estonian banks, newspapers and parliament. This paper explores the use of botnets as instruments of warfare. Seven scenarios are used to demonstrate how traditional applications of botnets such as spam, theft of resources and distributed denial-of-service attacks can have implications across the spectrum of warfare. Additionally, the paper discusses the ethical and political concerns associated with the use of botnets by nation states.

Keywords: National security, cyber warfare, botnets

1. Introduction

Cyber space, through its inextricable pervasiveness of all aspects of society, has significantly changed the nature of international and domestic conflict. Nation states find themselves at risk of attack and disruption through electronic means. Corporations are constantly defending against adversaries who seek to steal personal and proprietary information. Individual citizens are bombarded with unsolicited advertisements and malware on a daily basis. Although these threats manifest themselves in myriad ways, botnets have become the *de facto* tool of choice for hackers, organized crime groups and nation states [1, 3].

Interest in botnets has grown significantly. Although criminal activities receive the majority of attention, nation states have recognized the potential military applications. A real-world example is the distributed denial-of-service (DDoS) attacks launched against the nation of Estonia in 2007. Although the attacks were not directly attributed to a nation state, they underscore the impact that botnets can have on a nation's security. Indeed, botnets afford appealing attributes for the warfighting environment, including ease of setup, inherent command and control functionality, disruptive potential, high degree of anonymity and the ability to remain undetected [1, 4, 14].

Nuclear weapons are certainly not comparable to botnets in their scale and destructive potential, but they offer an interesting parallel. As instruments of warfare, nuclear weapons have a wide range of operational and strategic implications. We explore a similar notion by considering botnets as instruments of warfare. Specifically, we examine how traditional applications of botnets (e.g., spam, resource theft and DDoS attacks) can be leveraged to achieve operational and strategic objectives with respect to nation state conflicts. Example scenarios are provided that demonstrate how botnets can be used in conflicts between nation states. Also, ethical and political concerns associated with the use of botnets in conflict are discussed.

2. Background

A botnet consists of an "army" of host computers (bots) that have been infected by malware, typically unbeknownst to their owners. The malware installs a backdoor or communication channel that enables the bot to receive commands from an authoritative controller (botmaster). Bots typically attempt to compromise other machines until the botmaster issues a command to stop [1]. As a result, botnets can propagate rapidly and grow to include thousands, even millions of machines [3].

Botmasters use a command and control channel to issue commands to their bots. While various mechanisms exist, the two main types of command and control channels are peer-to-peer (P2P) protocols and Internet Relay Chat (IRC). In a P2P botnet, a bot behaves as a client and as a server. The architecture enables bots to directly relay commands among one another. To issue directives, an attacker selects a bot to serve as the botmaster and issues commands that propagate throughout the botnet. This structure is particularly difficult to stop and track because there is no fixed botmaster source [14].

IRC botnets leverage the scalability and flexibility of the IRC protocol to issue commands. In an IRC botnet, bots are directed to connect to specified botmaster servers periodically to receive commands, updates and other directives [1]. IRC botnets are easier to set up and maintain, but their command channels are centralized to specific servers, which make them easier to disable once detected. While IRC-controlled botnets are more common, P2P botnets and new variants are on the rise. Regardless of the command and control structure, botnets offer a high degree of anonymity and the ability to mask the underlying architecture. Indeed, without inspecting bot traffic, it is difficult to discern if individual bots are associated with a given botnet [1, 4].

The primary goal when establishing a botnet is to amass a large number of infected hosts without much consideration of the types of hosts. As a result, bots cannot be blocked or disabled without affecting the unknowing users of the compromised hosts. Additionally, preventing the compromise of host computers is extremely difficult. Even if users follow sound security practices, a large number of hosts are invariably exposed to infection.

Historically, botnets have been used to send spam and unsolicited advertisements [13]. Botmasters distribute large volumes of tailored advertisements on a fee-for-service basis using their subordinate bots to send email. Bots also have the ability to serve as data collection devices to obtain personal information for identity theft and other malicious activities [7].

From a warfare perspective, the best known tactic is to use a botnet to launch DDoS attacks. DDoS attacks seek to prevent legitimate users from accessing services by saturating the resources of the targeted machines. The large number of hosts and the anonymity associated with a botnet render it ideal for this type of attack. For example, a botmaster may direct subordinate bots to repeatedly connect to and synchronize with a networked computing resource. The attacks then generate massive amounts of traffic that limit the bandwidth available for legitimate users and overwhelm the target [1, 2, 8]. This tactic was demonstrated successfully in Estonia in April–May 2007 against targets that included government portals, banking sites and ATMs, emergency response services, root domain name servers and media portals. The botnet that launched the attacks apparently incorporated more than one million nodes across several countries, including the United States. Estonia was forced to block inbound international traffic in order to mitigate the attacks [2].

3. Botnet Warfare Scenarios

This section presents seven scenarios that leverage botnets as instruments of warfare. The scenarios are generic in nature and are not based on current or past events. The goal is to illustrate how various botnet capabilities might be used in support of strategic and operational objectives.

All the scenarios involve two fictional nation states, Atlantis and Lemuria. We assume that both nation states have a cyber infrastructure that is similar to that existing in industrialized countries. We also assume that the two countries are not bound by international restrictions such as those imposed by the Geneva Conventions, nor are they concerned with the political impact of their decisions. These assumptions permit the analysis to focus on botnet capabilities in the context of worse-case scenarios. The ethical and political issues related to botnet warfare are discussed in the next section.

Each botnet warfare scenario provides the overall objective, details of the tactical deployment of a botnet and the consequences of the attack. For reasons of clarity, the attacker is always Atlantis and the victim is always Lemuria. We also assume that Atlantis controls a botnet of significant scale that comprises a large number of bots within Lemuria.

3.1 Propaganda

The purpose of a propaganda attack is to influence the attitude of a group of individuals towards some cause or position. Propaganda typically has an essence of truth, but often uses selective facts to incite the desired emotional response. While typical delivery mechanisms include radio, television and print media, the widespread use of the Internet makes it attractive to disseminate propaganda using botnets.

- **Attack:** Atlantis directs the bots in Lemuria to download various forms of Atlantean propaganda from advertisement servers and display them to users. Computer configurations are altered so that website fetch requests are redirected to sites hosting Atlantean propaganda. Also, bots are used to send spam containing propaganda to large numbers of Lemurian users.

- **Effect:** The psychological effect of this type of attack is difficult to assess. However, the impact of a message delivered directly to individual users should not be underestimated. Consider the recent events in Egypt. Wael Ghonim, a Google marketing manager in Cairo, utilized Facebook to organize massive protests [12]. His ability to motivate and disperse a coherent message to a large populace is credited with helping force President Mubarak to step down. Indeed, with the Internet overtaking newspapers and approaching television as the main source of national and international news [10], the ability to leverage this outlet affords an opportunity to influence and control the views and perceptions of a large populace. Also, the fact that the Lemurian government has been unable to stop this attack may undermine its credibility. Lemuria could, of course, analyze Internet traffic to identify the primary servers that distribute the propaganda. However, stopping the attack completely would likely result in self-imposed denial of service.

3.2 Disinformation

In the intelligence domain, disinformation is the deliberate spreading of false information to mislead an adversary. Unlike propaganda that is designed to incite an emotional response, disinformation attempts to manipulate the audience by discrediting information or supporting false conclusions. Similar to propaganda, the widespread use of the Internet offers the ability to push disinformation to a massive population. Indeed, the ability to modify web pages or redirect users to sites without their knowledge offers the adversary a powerful means to manipulate individuals.

- **Attack:** Atlantis bots redirect their infected machines to connect to spoofed Lemurian media pages that provide false information on economic, political and health issues. Additionally, mass emails from spoofed Lemurian addresses provide information that supports the false web sites and discredits legitimate Lemurian media sources.

- **Effect:** As with the propaganda attack, the psychological toll of this scenario is difficult to gauge. However, the attack introduces a level of mistrust in the general population. While there is no guarantee that all

Lemurians will be affected, enough of the populace could be provided with false information to cause confusion and unrest. The legitimacy of Lemurian government policies, guidance and direction is likely to be questioned. Lemuria might respond to this attack by directing its citizens to rely on "trusted" media sources (e.g., television, newspaper and radio). However, it is likely that the attack would have political and psychological ramifications.

3.3 Conflict Instigation

This scenario creates a conflict between nation states for political, economic or military purposes. Instead of one nation directly attacking another nation state, the first nation state can use deception to provoke a third nation state to enter into a conflict with the second nation state. In this manner, the first nation state can achieve its ends without the perception of direct involvement.

- **Attack:** Atlantis directs its bots in Lemuria to begin DDoS attacks on systems that are critical to the government of Mu, a third nation state. Mu perceives the cyber attack as being instigated by Lemuria and threatens a response. Without diplomatic or international intervention, the situation may escalate.

- **Effect:** It is difficult to attribute the attack because of the anonymity associated with botnet channels. Indeed, Lemuria would most likely have to prove to Mu that it did not instigate the attack. If Lemuria cannot prove conclusively that the DDoS attacks were initiated by another actor, a tense stand-off or escalation is likely to occur.

3.4 Revenue Generation

The sale and lease of botnets for sending spam or harvesting data has become standard practice [11]. A small nation state can garner significant revenue from the use of its botnets. Indeed, terrorist organizations (although they are not classified as nation states) have already demonstrated the ability to use botnets to gather information and generate revenue to sustain their causes [15].

- **Attack:** Atlantis uses bots to disseminate "sponsored" adware and deploy information-gathering malware (e.g., keylogging software). Atlantis receives payment from commercial entities to distribute advertisements and sells the data obtained via keylogging software on the black market. The generated revenue is discreetly added to Atlantis' treasury.

- **Effect:** Even if Lemuria becomes aware of the operation, the options for mitigation are quite limited. This is even more problematic if the operation is launched from multiple countries. Lemuria can appeal to the international community for assistance, but even then, the options are limited because of the difficulty of attributing botnet attacks.

3.5 Service Disruption

The effects of a service disruption attack range from intermittent degradation of service to complete denial of service. A subtle attack may degrade a service by slowing it down periodically so that it cannot be trusted. The targets can include control systems, telecommunications systems and banking systems. Although botnets primarily impact networks and services, botmasters can instruct their subordinate bots to disrupt or disable (e.g., reformat) their host machines.

- **Attack:** Atlantis launches DDoS attacks against government utilities, banking websites and other high-traffic Internet portals in Lemuria. The initial wave of attacks constitutes a "show of force" to demonstrate Atlantis' capabilities to the Lemurian people. The intensity and scope of attacks are gradually increased until Lemuria is forced to concede to Atlantis' demands.

- **Effect:** The effect of this type of attack may range from annoyance to widespread fear and confusion. Initial attacks against specific resources (e.g., popular web pages or media outlets) may serve as a mechanism to anger and frustrate the populace. As the conflict wears on, the attacks may escalate to disrupt critical infrastructure assets. Service disruption attacks may also be used as a diversionary tactic while offensive actions are performed in other areas. Few options are available for dealing with widespread DDoS attacks. Blocking inbound international traffic (as Estonia did in 2007) may not help if a large number of bots with the ability to autonomously launch DDoS attacks are deployed within Lemuria.

3.6 Intelligence Exfiltration

Gaining intelligence on the enemy is paramount in any conflict; relevant and timely information can be the difference between the success and failure of a military operation. Military operations have become highly dependent on technology and the Internet. This reliance makes them susceptible to the same types of attacks that criminal organizations currently use against individuals. For example, bots often function as data collection devices that harvest personal information. Similarly, bots injected into a military network can serve as a large, distributed data collection tool to gain intelligence and situational awareness about current and future military operations.

- **Attack:** Atlantis deploys bots in Lemurian military and military-related commercial networks. The bots remain dormant until commanded to support contingency operations, at which time they monitor and search for files containing sensitive information (e.g., about public officials, state activities and military plans). These files are transmitted to Atlantean servers for analysis.

- **Effect:** If Lemuria detects the exfiltration, it can leverage the attack by feeding false information to Atlantis. This is effective only to the extent that Lemuria can detect and control the exfiltration. However, Lemuria may not be able to trust the integrity of its networks and may have to take them down so that they can be reconfigured. Not detecting the exfiltration could result in serious consequences for Lemuria.

3.7 Chaos Instigation

A coordinated campaign involving different types of botnet attacks can cause widespread chaos. Indeed, considerable damage could be wrought without deploying a single military unit.

- **Attack:** Atlantis initiates a misinformation campaign focused on political and economic targets in Lemuria. Simultaneously, a propaganda initiative is launched that highlights the lack of control that the Lemurian leadership has over its assets. Atlantis warns the Lemurian populace of dire consequences if its demands are not met. Atlantis then launches massive DDoS attacks against Lemurian critical infrastructure assets by instructing its Lemurian-based bots to disable their host machines.

- **Effect:** Lemuria must deal with the fear that the attacks generate among its populace and mitigate the effects of the attacks on its critical infrastructure assets. Because the attacks are launched from within and outside its borders, there is little that Lemuria can do aside from disconnecting its key assets from the Internet. This may actually exacerbate the problem and amplify the effects of the attacks. The attacks may become so debilitating that Lemuria may consider kinetic retaliatory strikes. Absent overwhelming proof – which is difficult to obtain because of the attribution problem – Lemuria may be hard-pressed to retaliate, especially if Atlantis emphatically denies a hand in the attacks.

4. Ethical and Political Issues

The scenarios presented in the previous section ignore ethical and political concerns that may impose significant barriers to launching botnet attacks. This section examines the major ethical and political consequences associated with the use of botnets as an instrument of warfare.

The first major issue concerns the Geneva Convention and its implications. Compromising a computer and installing botnet malware is equivalent to unauthorized seizure. If the compromised computer belongs to a civilian entity, the action could potentially be deemed an attack on non-combatants. An attack on civilian-owned property is strictly prohibited under Protocol I, Article 52 of the Geneva Convention [5]. Although the term "attack" may not withstand international scrutiny, a computer compromise could be deemed as an attack if it impacts critical infrastructure assets and, therefore, endangers civilian lives. Attacks on resources that are not identified as key military objectives and disrupt civilian life are proscribed by Protocol I, Article 54 [5]. A nation state that uses its own citizens' computers to launch botnet attacks on another country could be deemed to be using "human shields" – an action that is prohibited under Protocol I, Article 51 of the Geneva Convention [5]. Furthermore, any computers that are used in an offensive manner can be considered to be weapons of war and, as such, the operators of these computers can be labeled as combatants. However, because of the attribution problem, the controlling computers and their operators could be in doubt; this could potentially draw unwitting civilians into the conflict.

Attribution is a paramount issue. Botnets are complex with shadowy command and control structures, making the identification of a botmaster extremely difficult. Identifying the real perpetrator of an attack is even more complicated when botnet resources are "outsourced" to third parties.

Few legal cases address the use of botnets. Microsoft recently won a legal battle against the Waledac spam botnet via an *ex parte* judicial procedure [9]. The botmaster was never determined or located; however, the primary web domains used in Waledac's command infrastructure were identified. The *ex parte* procedure enabled the court to forcefully transfer control of these domains to Microsoft, effectively shutting down the ability of the botmaster to relay commands to the bots. While this exact situation may not be applicable to all botnets, it presents a means to defend against botnets within the scope of law instead of using purely technical approaches.

Another recent incident involved the U.S. Department of Justice and the FBI dismantling the Coreflood botnet [6]. In this incident, commands were sent to the infected hosts to force them to stop communicating with the botmaster. This case is unprecedented in that government officials sent commands that altered the behavior of computer systems without their owners' knowledge or consent. It would be interesting to see if this approach would withstand legal scrutiny.

At the heart of many of these issues are the lexicon and classification relating to the use of botnets in warfare. International provisions and agreements that specifically cover network attacks would be a significant help. It is necessary to clarify the status of machines and the owners of the machines that are used to perpetrate attacks. Also, classifying attacks according to capabilities would help define the appropriate responses. For example, is a botnet attack that disrupts the power grid an "armed" attack? If so, how does the victim respond?

A vital issue that must be addressed pertains to attacks by non nation state actors. While political constructs and international law may prevent many nation states from launching botnet attacks, history has shown that terrorist organizations and other radical groups have no such restrictions. It is critical that nations reach agreement on the protocols for dealing with attacks by non nation state actors before such scenarios actually play out.

5. Conclusions

Botnets can be used as instruments of warfare to achieve strategic and operational objectives. With few direct defensive measures available, botnets can disrupt operations in government and industry, and impact the populace by targeting critical infrastructure assets. The ethical and political implications of botnet use are significant. Currently, the attacks are too indiscriminate for botnets to be considered as legitimate weapons under international law and conventions. Nevertheless, the role that botnets play in conflict can be expected to increase. Nation states must assess the retaliatory options and be prepared to respond if and when botnets are used against them.

The attack scenarios demonstrate the depth and breadth of the offensive capabilities that botnets afford in a wartime environment. Additional research is required to develop viable legal, policy and technical solutions for detecting, preventing and responding to botnet attacks. Until holistic defensive strategies are in place, nations will be ill-prepared to deal with the full impact of botnet attacks.

Note that the views expressed in this paper are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Department of Defense or the U.S. Government.

References

[1] M. Bailey, E. Cooke, F. Jahanian, Y. Xu and M. Karir, A survey of botnet technology and defenses, *Proceedings of the Cybersecurity Applications and Technology Conference for Homeland Security*, pp. 299–304, 2009.

[2] L. Brooks, Botnets: A Threat to National Security, M.S. Thesis, Department of Computer Science, Florida State University, Tallahassee, Florida, 2008.

[3] A. Cole, M. Mellor and D. Noyes, Botnets: The rise of the machines, *Proceedings of the Sixth Annual Security Conference*, 2007.

[4] M. Feily, A. Shahrestani and S. Ramadass, A survey of botnet and botnet detection, *Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies*, pp. 268–273, 2009.

[5] International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), International Humanitarian Law – Treaties and Documents, Geneva, Switzerland (www.icrc.org/ihl.nsf/full/470?opendocument), June 8, 1977.

[6] D. Kaplan, Coreflood-style takedowns may lead to trouble, *SC Magazine*, April 15, 2011.

[7] J. Leonard, S. Xu and R. Sandhu, A framework for understanding botnets, *Proceedings of the Fourth International Conference on Availability, Reliability and Security*, pp. 917–922, 2009.

[8] S. Liu, Surviving distributed denial-of-service attacks, *IT Professional*, vol. 11(5), pp. 51–53, 2009.

[9] E. Mills, Microsoft legal punch may change botnet battles forever, *CNET News* (news.cnet.com/8301-27080_3-20015912-245.html), September 9, 2010.

[10] Pew Research Center for the People and the Press, More young people cite Internet than TV – Internet gains on television as public's main news source, Washington, DC (people-press.org/reports/pdf/689.pdf), January 4, 2011.

[11] B. Prince, Botnet for sale business going strong, security researchers say, *eWeek.com* (www.eweek.com/c/a/Security/BotnetBotnet-for-Sale-Business-Going-Strong-Security-Researchers-Say848696), October 25, 2010.

[12] C. Smith, Egypt's Facebook revolution: Wael Ghonim thanks the social network, *Huffington Post*, February 11, 2011.

[13] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel and G. Vigna, Your botnet is my botnet: Analysis of a botnet takeover, *Proceedings of the Sixteenth ACM Conference on Computer and Communications Security*, pp. 635–647, 2009.

[14] P. Wang, L. Wu, B. Aslam and C. Zou, A systematic study of peer-to-peer botnets, *Proceedings of the Eighteenth International Conference on Computer Communications and Networks*, 2009.

[15] C. Wilson, Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, CRS Report for Congress, RL32114, Congressional Research Service, Washington, DC, 2008.