FireEye: Taking the Botnet Threat Seriously

A White Paper Prepared for FireEye
October 2007

Table of Contents

Executive Summary

Security has been a standard feature of IT for many years now, yet a pernicious threat continues to spread, with an impact felt by individuals, businesses and national governments alike. That threat is the botnet (for networks of bots, or compromised machines), a chimera of multiple functionalities that integrates compound malware threats and a remarkable range of functionality with remote network command-and-control. Why have botnets been so successful? In large measure because traditional defenses address the threat in pieces and parts—as malware, as network threat, as social engineering exploit—requiring enterprises to depend on the capability (and goodwill) of individuals to practice "safe computing."

None of these address the botnet threat as a whole. Botnets are more than the sum of their parts. They are more than malware, more than the "bots" that are simply the agents for their distributed functionality. They are complex attack platforms that have become the preferred means for posing some of the most dangerous threats in the connected world—threats that recent events suggest may pose substantial risks, not just to individuals but to enterprises and network service providers, beyond IT and information security alone.

Into this atmosphere, FireEye has entered with a new and distinctive approach to the complex challenges of botnet defense. With a package of functionality that factors in the characteristics of botnets themselves, FireEye leverages virtualization to identify and isolate threats to actual network endpoints, but it does so in a way that isolates the threat from the endpoint itself. This enables FireEye to capture real-world botnet activity, but in a safe environment insulated from IT and information assets at risk. To this mix FireEye adds something that raises this new approach to botnet defense to a higher level: a global intelligence network that links FireEye-defended networks in a defensive architecture that spans multiple networks, just as botnets do themselves.

The escalating stakes of digital defense increasingly demand that this egregious threat be taken more seriously, not just by enterprises, but by network service providers as well, since the scale and scope of any individual botnet—let alone the threat as a whole—is most often quite literally worldwide. It may not be too much to anticipate that authorities may one day demand the same level of quality for security across multiple networks that they already require of the network services on which the public good depends.

In this paper, Enterprise Management Associates (EMA) takes a look at how the botnet threat became so serious, how botnet defense must answer the challenge, and how FireEye introduces a new approach to anti-botnet protection that more fully recognizes their comprehensive nature and scope. Executives will gain a new appreciation for the true scale of the botnet threat, and how today's emerging solutions must answer the threat with a similar level of multi-faceted defense.

The Botnet Threat: How Did Things Ever Get This Bad?

IT has been subjected to a number of security plagues in recent years, but few of them have the potential for widespread havoc of the botnet, a category of threat that has raised the risk of coordinated, distributed attack to a new level—one that seems to have been poorly anticipated not just by IT shops, but by enterprises, network service providers, and perhaps even governments—worldwide.

A botnet is comprised of a collection of machines that have been infiltrated by functionality that can be automated and controlled remotely by an attacker. The attack traces its roots to automated Internet Relay Chat (IRC) agents known as "bots" (short for "ro*bots*"), easily available and easily deployed, and originally intended to extend and automate the management of IRC networks. The remote control capabilities of bots enable them to be leveraged in a coordinated manner to unleash attacks against networks as well as targeted, stealthy attacks on specific servers via agents managed remotely from a command-and-control (C&C) center operated by one or more attackers (hence bot*net*). The subversion of each individually exploited system is often invisible to its user, and may be spread using techniques from phishing to Trojan infiltration to direct network exploit and the self-propagation capabilities of worms. Not infrequently, all of these techniques may be used in combination to propagate bots, in so-called blended or compound threats.

A botnet can be used by an attacker or group of attackers in a number of ways. It can be used to trigger a distributed denial-of-service (DDoS) attack that overwhelms a

target (e.g., Web site) with traffic generated from a large number of bot-infested victim machines. It can be used to transmit and amplify spam. It can harvest sensitive information not only from large numbers of victims, but also from the resources with which victims interact. All of these capabilities have obvious tangible value: as a mercenary attack platform; in spam generation for hire; or in the large-scale theft of sensitive information directly linked to tangible assets, such as financial account information or high-value intellectual property. For all these reasons—particularly as digital exploits become more attractive to organized crime—the botnet is becoming an increasingly threatening form of attack.

Why have botnets become so successful? In part because conventional defenses deal with one piece or another of the threat, but do not address the botnet threat as a whole. For example, viewed in one sense, bots are often seen as simply another form of malware (*mal*icious soft*ware*). While this is only partly true (botnets also have substantial network, command-and-control, and human intelligence aspects), this narrow perception has led to an emphasis on anti-malware techniques such as anti-virus, anti-spyware and anti-spam for controlling botnet penetration.

Network security measures target another piece of the botnet threat. Network defenses such as firewalls and intrusion detection and prevention (IDS/IPS) systems have become commodity, even in the home, as the standard means of defending against network threats—yet botnets proliferate regardless. Why?

One of the weakest aspects of defense becomes apparent when considering that businesses and private individuals alike are encouraged simply to practice "safe computing"—to "just say no," as it were, to questionable messages or unfamiliar attachments that could unleash a bot attack or execute other threats, no matter how genuine they may appear. The limitations of today's defenses in many environments coupled with the desire not to interfere with individual productivity means that this approach still prevails, despite the fact that attackers are becoming more sophisticated in crafting credible social engineering exploits all the time.

These are all common and widely practiced forms of IT defense. Each has a measure of effectiveness against certain aspects of the botnet threat. Millions of businesses and individuals employ these measures.

And yet, in spite of pervasive IT security tools, millions of systems have been compromised by bots regardless. They command far more systems than many today imagine. The threat known as Storm has by itself been estimated to have infected as many as 10 million machines—and that is just *one* type of bot. Various sources estimate the number of bot-infested machines to be as high as 150 million, collectively making botnets by far the most pervasive form of distributed computing ever extended throughout the Internet. In contrast, the SETI@Home project, a search for evidence of extraterrestrial intelligence leveraging volunteer systems, has been estimated to have engaged over 5 million participants worldwide. SETI@Home may have been the largest *legitimate* grid ever attempted—but as a whole, botnets make such efforts pale by comparison.

Today, the scope and scale of botnet capability is becoming more manifestly apparent. As a platform for systematic attack, botnets have been implicated in efforts to exploit leading-edge application architectures, such as a recently reported botnet attack on eBay, an online leader. The irony of the alleged eBay case is that it blends what in the past may have been a crude form of attack—brute force "lockpicking" based on trial and error—into a sophisticated and systematic effort to exploit weaknesses in XML structures and Service Oriented Architecture—touted by many as the future of IT. The result has reportedly been the systematic exploitation not only of eBay, but of its customers, and even payment providers such as eBay's own PayPal service—an incident that is nothing short of a fire alarm for online business at every level.

Equally disconcerting is the ability of botnets to infiltrate and take advantage of major enterprises, despite their ability to invest in state-of-the-art defense. The brand damage risk arising from the inability to protect environments trusted to be among the safest in the world from the botnet threat is incalculable, as in the alleged case of an infiltration of Pfizer's network to amplify spam, including spam that "promotes" the company's own products—alongside less savory items.

These factors are why law enforcement agencies have specifically targeted the botnet threat on a national level, as with the US Federal Bureau of Investigation's "Operation Bot Roast." The scale of the threat is illustrated by a recent DDoS attack unleashed throughout

the nation of Estonia, and is implicit in the international scope of events ranging from alleged infiltrations of military installations worldwide, to the specter of cyberterrorism.

Addressing the Gaps in Existing Approaches

If defense is ever to gain on the botnet threat, it must first of all recognize that a botnet is more than the sum of its parts. It is not simply a collection of bots. Nor are bots merely malware. Bots are the agents of a botnet, a well-organized, distributed attack platform with command-and-control and multiple functionalities, each one posing its own set of containment challenges. A botnet makes the most of polymorphism in what is effectively a grid, and then some. It is one of the most fluid and mobile computing environments in existence.

Behavior-recognition technologies have been touted as the next generation of both anti-malware and network defense, and have sometimes been identified as a potentially suitable weapon in botnet defense. But these technologies have often been challenged in recognizing variants in behavior that can lead to high numbers of both false positives and false negatives. The challenge is compounded when applied to botnets, which are among the most dynamic changelings known to IT security. Bots can be polymorphic in the extreme, shipped as packages containing multiple varieties of functionality and able to call on any combination that fits the need. Botnet polymorphism extends beyond the behavior of bots themselves. Botnets leverage advanced techniques in network detection avoidance, such as "fast-flux" domain name services (DNS) that update records of botnet command and control (C&C) nodes so fast that they become exceedingly difficult to trace, let alone shut down.

Effective anti-botnet protection requires more than just breaking down silos between malware defense and network security tactics. There is also a human component that drives the command and control of the botnet itself. Bots are not limited by their own automation capabilities in choosing a polymorphic variant, for example; remote manual control can shape the characteristics of a botnet as well. Botnet managers can also avoid detection by "herding" bots rapidly from one set of victimized hosts to another, with the result that, by the time botnet nodes have been well identified, they may no longer be active. Fast-flux DNS and the use of multiple proxies (often bots essentially proxying each other), and techniques such as single-use URLs make such tactics possible, placing substantial barriers in the way of finding current, active control nodes in constant motion.

This human control element requires an equal level of intelligence on the part of botnet defense, one attuned to the unique aspects of the botnet challenge, and having the visibility across multiple networks available to botnets themselves. This intelligence also requires a *realistic* perception of botnet activity. For example, botnet intelligence efforts have included techniques such as the use of decoy networks—so-called "honeynets"—to capture and identify bots and botnet characteristics. Honeynets often leverage so-called "dark" networks of address spaces not allocated to actual use. The advantage of the "dark net" approach is that many bots—as well as blended or compound attacks—have often been indiscriminate in scanning and identifying potential targets. Using a dark net as a honeynet also avoids exposing live or "lit" net nodes. However, botnet herders are becoming increasingly sophisticated in identifying dark nets by their lack of response—or by a response indicative of a honeynet—and can therefore be expected to increasingly avoid them. As botnets continue to grow in sophistication, dark net techniques could become more limited—but exposing lit nets poses risks to live production systems that must be contained.

Of course, one of the largest gaps in defense—against not only botnets but other forms of attack as well—is the fact that far too much still depends on the actions of people. Phishing has become one of the most popular techniques of all for delivering a threat. So long as defense depends on the ability of people to recognize a threat and take appropriate action, attacks will always have a fighting chance. Today, phishing efforts are designed to look as convincing as possible, with so-called "spearphishing" attacks targeting specific groups of potential victims. Even highly skilled experts can have trouble distinguishing such an attack from a legitimate message or other communication. Effective defense means moving recognition and containment to a more reliable level—a level that can only have an impact when the detailed analysis of widespread threats is automated in purpose-designed defense systems. Nowhere is this more necessary than in service provider networks, which

serve the millions of private individuals on whose unfortunate actions botnet proliferation often depends.

In short, botnet defenses need to leverage many of the same advantages enjoyed by botnets themselves:

- They must combine automated recognition with human intelligence and control. In particular, they must move control away from dependence on the abilities of ordinary users and potential victims, and put it instead into the hands of automated, accurate recognition capabilities reinforced by botnet-attuned intelligence.
- In order to provide the most accurate detection and intelligence, they must consider leveraging live or "lit" network nodes to capture real-world botnet behavior—but they must do so without exposing live networks to even greater risk.
- They must have visibility into the dynamic fluidity of botnets as they move and change, able to detect highly polymorphic functionality across multiple points of visibility and control in multiple networks. This requires defense *across* enterprises and network service providers, not just within the enterprise or provider network alone.

The FireEye Difference

With its distinctive focus on anti-botnet protection, FireEye introduces a new class of IT security solution that seeks to answer each of these challenges of the multi-dimensional botnet threat.

FireEye begins with leveraging virtualization for real-time capture of actual attacks on lit networks, but in a safe environment isolated from actual lit nodes. The FireEye Botwall™ solution virtualizes entire endpoint systems in a network appliance form factor. To the attacker, the FireEye platform looks identical to actual nodes on a lit net. From the perspective of the protected network, FireEye captures and analyzes live botnet activities in a safe environment isolated from live production systems. This enables the FireEye Botwall to capture botnet activity such as botnet propagation attempts, C&C locations and unauthorized bot communications, all within a virtualized victim machine that performs as a real endpoint while protecting the actual endpoint itself.

This allows FireEye to deploy its solution at the level of the network, away from high-risk defense centered on the endpoint itself, where user behavior as well as the hidden nature of rootkits and kernel-level threats may defeat endpoint-level security functionality. This also helps remove the risks introduced when defense depends on the actions of individual users, giving the enterprise or network service provider more direct control over botnet risks.

FireEye has, however, gone beyond the level of the individual network, and has recognized the potential of coordinating the intelligence of FireEye Botwall systems across multiple enterprise and service provider networks for giving wider visibility into the movements of botnets themselves. The FireEye Botwall Network then disseminates and shares this intelligence back to

Figure 1: The FireEye Botwall product family scales to meet the requirements of a wide range of organizations.

FireEye systems deployed throughout FireEye's customer base. Because FireEye systems virtualize actual lit net behavior, the FireEye Botwall Network can accurately identify and track the movements of botnets across multiple FireEye customers, thus providing insight into the activities of actual botnets, and more current and realistic awareness of botnet behavior. This, in turn, enables FireEye customers to benefit from the deployment of FireEye systems throughout both public networks and private enterprises, designed to support defense with a scale of visibility and intelligence on par with botnets themselves.

This combination represents a different approach that more fully recognizes the nature of today's more serious distributed threats. With a distinctive approach to leveraging actual endpoint functionality in a safely virtualized environment, a package that deploys this endpoint functionality in a network form factor, and the widespread visibility of FireEye control points across multiple enterprise and service provider networks, the FireEye solution embraces more of the comprehensive scope of the botnet threat than traditional approaches, and recognizes that today's distributed attack platforms are more than malware, network threats, social engineering, or polymorphic functionality alone.

EMA's Perspective

Recent attacks such as the Estonian DDoS outbreak and the spread of Storm ought to be more than just indicators of a new type of threat. They should be seen in the light of recent indications that organized groups are targeting gaps in the defense of resources critical not only to IT, but to society as a whole. Some of these events may even indicate that information warfare may be a more real possibility than many have considered to date, as suggested by reports of recent and seemingly organized intrusions into high-sensitivity military installations.

Neither enterprises nor network service providers should disregard the implications of these events. Malicious parties will of course leverage the most effective platform from which to mount a well-organized attack. This means that botnets should be recognized for what they are. They are not simply just another form of attack. Together they are one of the most widespread and successful distributed computing efforts ever attempted. How, then, to get a handle on a threat that can be found virtually anywhere, where distributed nodes can easily change form or appear and disappear without reducing the threat itself?

Networks may want to consider how similar those characteristics are to those of Internet Protocol (IP)

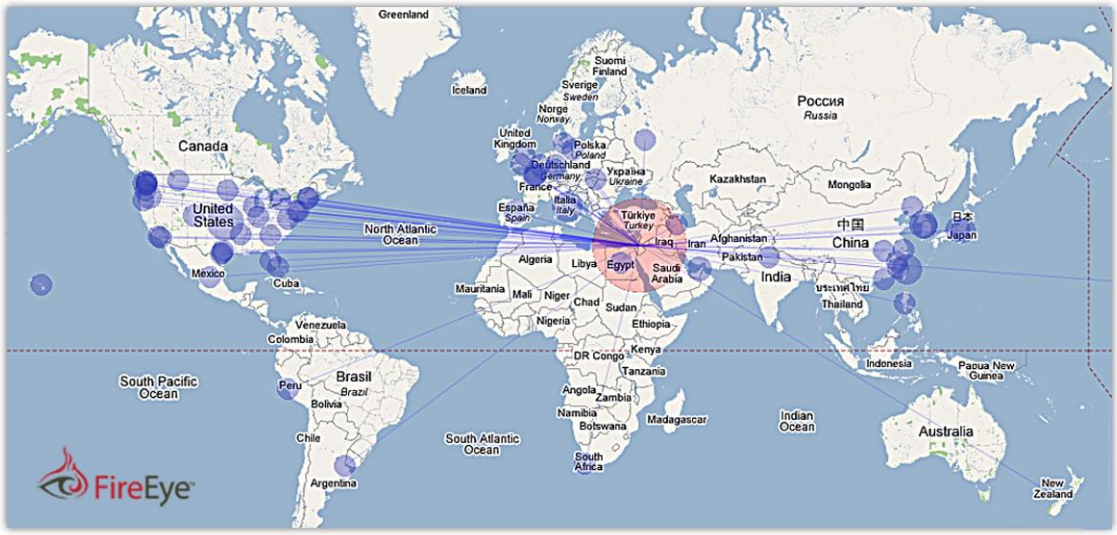

Figure 2: Illustration of the FireEye Botwall Network tracking a botnet, centered in this case in the Middle East. The comprehensive FireEye solution follows botnet activity as it moves and changes—a key value to countering one of today's most dynamic threats.

networks. IP networks were expressly designed to be "bulletproof," able to sustain the loss of nodes in the network or changes that affect network topology with minimal impact on the network as a whole. Botnets share many of these same qualities: They are widely distributed and offer multiple paths of communication between nodes that support survivability.

Network service providers and enterprises have learned how to harness these capabilities in the assurance of priorities such as quality-of-service (QoS). Perhaps a lesson can be drawn from that experience. As law enforcement agencies such as the FBI seek to gain more effective control of the botnet threat, the assurance of security against such threats may well become an aspect of a network service quality that regulators take more seriously—particularly among the network and Internet service providers that serve the millions of individuals targeted by the phishing and social engineering attacks on which botnet proliferation often depends.

FireEye has introduced a way for enterprise networks and service providers alike to address this threat, in a way that reflects the cooperation that currently exists among networks to assure service priorities that are either mutually beneficial or mandated by law. With a distinctive set of capabilities such as the shared intelligence of its global Botwall Network, FireEye offers these networks a new approach to one of the most substantial challenges in IT security. It features an innovative capability set that leverages the advantages of virtualization in using lit nets to capture botnet activity, but in a way that provides a measure of insulation against attack for potential botnet targets, and which helps relieve the enterprise from too great a dependence on the actions of individuals and the vulnerabilities of endpoints for its own safety.

EMA suggests that service providers and networks of all sizes may want to consider these parallels with what regulators currently require of public networks for the public good, and how a new generation of security solutions that target the botnet threat specifically could have an impact on what IT security looks like in a future not too far distant, when—not if—the botnet threat becomes an even higher priority for regulators, law enforcement agencies, and military defense.

About FireEye

FireEye, Inc. is the leader in anti-botnet protection, enabling organizations to protect critical intellectual property, computing resources, and network infrastructure against bot infiltration. Today's most damaging attacks originate from and through highly organized botnets, or networks of remotely controlled, compromised machines. FireEye delivers a complete solution that is designed from the ground up to detect and protect organizations from botnets through global and local intelligence and analysis. The company is backed by Sequoia Capital, Norwest Venture Partners, and JAFCO. For more information, contact (650) 543-1600 or email: info@fireeye.com. Visit FireEye at www.FireEye.com.

About Enterprise Management Associates, Inc.

Enterprise Management Associates is an advisory and research firm providing market insight to solution providers and technology guidance to Fortune 1000 companies. The EMA team is composed of industry respected analysts who deliver strategic awareness about computing and communications infrastructure. Coupling this team of experts with an ever-expanding knowledge repository gives EMA clients an unparalleled advantage against their competition. The firm has published hundreds of articles and books on technology management topics and is frequently requested to share their observations at management forums worldwide.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

1446.100907