BOTNET - Threats And Countermeasures

Saoud Sarwar[1] Ahmad Majeed Zahoory[2] Almas Zahra[3] Syed Mohd Tariq[4] Adil Ahmad[5]
[1,2,3,4,5]Department of Computer Science
[1,2,3,4,5]Al-falah School of Engg. & technology, Faridabad, India

Abstract — Robot networks, popularly known as botnets, have a varied history. In essence, a bot is simply a series of scripts or commands or a program that is designed to connect to something (usually a server) and execute a command or a series of commands. Essentially it performs various functions. It needn't be malicious or harmful.
Bots and their uses have evolved from the simple channel or game watchers (for example, Wisner's Bartender and Lindahl's Game Manager bots) to providing specialized services such as managing databases or maintaining access lists. This report covers a very different use: the "herding" of bots (also called drones or zombies) by cybercriminals to support their criminal activities.
As they affect corporations, these criminal activities can include stealing trade secrets, inserting malware into source code files, disrupting access or service, compromising data integrity, and stealing employee identity information. The results to a business can be disastrous and lead to the loss of revenue, regulatory compliance, customer confidence, reputation, and even of the business itself. For government organizations, the concerns are even more far reaching.
We will look at how criminal bots have evolved, the industry that supports their creation and distribution, and how they are used today by various cybercriminal groups. We will also suggest where we believe bots are headed in the near future.
*Keywords:*BOTNET, Zombie, DDoS, Spyware, Malware, Adware and Phishing.

I. INTRODUCTION

A BOTNET is an army of compromised machines, also known as "zombies," that are under the command and control of a single "botmaster". The rise of consumer broadband has greatly increased the power of botnets to launch crippling denial of service (DoS) attacks on servers, infect millions of computers with spyware and other malicious code, steal identity data, send out vast quantities of spam, and engage in click fraud, blackmail, and extortion. BOTNET are the primary security threat on the Internet today. It is easy to commission botnet attack services and hackers are quicker than ever to exploit new vulnerabilities. Tens of thousands of machines are typically part of a single botnet. BOTNET are hard to detect because they are highly dynamic in nature, adapting their behavior to evade the most common security defenses.

II. HOW IS BOTNET CREATED

Botnet creation begins with the download of a software program called a "bot" (for example, IRCBot, SGBot, or AgoBot) along with an embedded exploit (or payload) by an unsuspecting user, who might click an infected e-mail attachment or download infected files or freeware from peer-to-peer (P2P) networks or malicious Websites.
Once the bot and exploit combination is installed, the infected machine contacts a public server that the botmaster has set up as a control plane to issue commands to the botnet. A common technique is to use public Internet Relay Chat (IRC) servers, but hijacked servers can also issue instructions using Secure HTTP (HTTPS), Simple Mail Transfer Protocol (SMTP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) strings. Control planes are not static and are frequently moved to evade detection; they run on machines (and by proxies) that are never owned by the botmaster.
Using the control plane, the botmaster can periodically push out new exploit code to the bots. It can also be used to modify the bot code itself in order to evade signature-based detection or to accommodate new commands and attack vectors.
Initially, however, the botmaster's primary purpose is to recruit additional machines into the botnet. Each zombie machine is instructed to scan for other vulnerable hosts. Each new infected machine joins the botnet and then scans for potential recruits. In a matter of hours, the size of a botnet can grow very large, sometimes comprising millions of PCs on diverse networks around the world. Figure 1 shows a typical botnet.

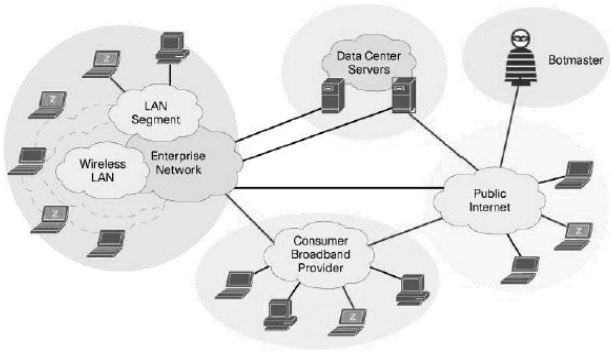

Fig. 1: A Typical Botnet with Zombies

Armed with this zombie army, the botmaster is now ready to launch the first major attack. Practically anyone with a computer is an attack target, whether a small business, a home user, a corporate office, or a retail point-of-sale terminal. Locating the botmaster is an extremely tricky task. The botmaster typically proxies the control commands through several compromised machines on diverse networks. Proxy connections, as well as the control plane, are changed often to make it nearly impossible to track down the botmaster.

A. The Impact of Botnets

Botnet-led exploits can take many forms.

1) Distributed Denial of Service (DDoS) Attacks

With thousands of zombies distributed around the world, a botnet may launch a massive, coordinated attack to impair or bring down high-profile sites and services by flooding the connection bandwidth or resources of the targeted system. Multigigabit-per-second attacks are not uncommon. Most common attack vectors deploy UDP, Internet Control Message Protocol (ICMP), and TCP SYN floods; other attacks include password "brute forcing" and application-layer attacks.

Targets of attack may include commercial or government Websites, e-mail services, Domain Name System (DNS) servers, hosting providers, and critical Internet infrastructure, even antispam and IT security vendors. Attacks may also be directed toward specific political and religious organizations, as well as gambling, pronography, and online gaming sites. Such attacks are sometimes accompanied by extortion demands.

2) Spyware and Malware

Zombies monitor and report users' Web activity for profit, without the knowledge or consent of the user (and at times for blackmail and extortion). They may also install additional software to gather keystroke data and harvest system vulnerability information for sale to third parties.

3) Identity Theft

Botnets are often deployed to steal personal identity information, financial data, or passwords from a user's PC and then either sell it or use it directly for profit.

4) Adware

Zombies may automatically download, install, and display popup advertising based on a user's surfing habits, or force the user's browser to periodically visit certain Websites.

5) E-Mail Spam

Most of today's e-mail spam is sent by botnet zombies.

6) Click Fraud

The exploit code may imitate a legitimate Web browser user to click on ads for the sole purpose of generating revenue (or penalizing an advertiser) for a Website on pay-per-click advertising networks (such as Google Adwords).

7) Phishing

Zombies can help scan for and identify vulnerable servers that can be hijacked to host phishing sites, which impersonate legitimate services (e.g., PayPal or banking Websites) in order to steal passwords and other identity data.

III. BOTNET DETECTION AND MITIGATION

Botnets use multiple attack vectors; no single technology can provide protection against them. For instance, the goal of a DDoS attack is to cripple a server. The goal of a phishing attack is to lure users to a spoofed Website and get them to reveal personal data. The goal of malware can range from collecting personal data on an infected PC to showing ads on it or sending spam from it. A defense-in-depth approach is essential to detect and mitigate the effects of botnets.

Traditional packet filtering, port-based, and signature-based techniques do not effectively mitigate botnets that dynamically and rapidly modify the exploit code and control channel, resort to "port-hopping" (or using standard HTTP/S ports such as 80 and 443), and shuffle the use of zombie hosts.

A variety of open source and commercial tools are currently used for botnet detection. Many of them analyze traffic flow data reported by routers. Others use behavioral techniques; for example, building a baseline of a network or system under "normal" conditions and using it to flag abnormal traffic patterns that might indicate a DDoS attack. DNS log analysis and "honeypots" are also used to detect botnets, but these techniques are not always scalable.

The most common detection and mitigation techniques include:

A. Flow data monitoring:

This technique uses flow-based protocols to get summary network and transport-layer information from network devices. Network Tools is often used by service providers and enterprises to identify command-and-control traffic for compromised workstations or servers that have been subverted and are being remotely controlled as members of botnets used to launch DDoS attacks, perform keystroke logging, and other forms of illicit activity.

B. Anomaly detection:

While signature-based approaches try to have a signature for every vulnerability, anomaly detection (or behavioral approaches) try to do the opposite. They characterize what normal traffic is like, and then look for deviations. Any burst of scanning activity on the network from zombie machines can be detected and blocked. Anomaly detection can be effectively used on the network as well as on endpoints (such as servers and laptops). On endpoints, suspicious activity and policy violations can be identified and infections prevented.

C. DNS log analysis:

Botnets often rely on free DNS hosting services to point a sub domain to IRC servers that have been hijacked by the botmaster, and that host the bots and associated exploits. Botnet code often contains hard-coded references to a DNS server, which can be spotted by any DNS log analysis tool. If such services are identified, the entire botnet can be crippled by the DNS server administrator by directing offending sub domains to a dead IP address (a technique known as "null-routing"). While this technique is effective, it is also the hardest to implement since it requires cooperation from third-party hosting providers and name registrars.

D. Honeypots:

A honeypot is a trap that mimics a legitimate network, resource, or service, but is in fact a self-contained, secure, and monitored area. Its primary goal is to lure and detect malicious attacks and intrusions. Effective more as a surveillance and early warning system, it can also help security researchers understand emerging threats. Due to the difficulty in setup and the active analysis required, the value of honeypots on large-scale networks is rather limited.

