Botnets: The New Threat Landscape

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.

Botnets 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. Botnets are hard to detect because they are highly dynamic in nature, adapting their behavior to evade the most common security defenses.

IT security teams must prevent corporate devices from becoming part of a botnet and protect corporate resources from botnet attacks. This white paper discusses the typical lifecycle of a botnet, the damage caused by botnet attacks, and the most effective detection and mitigation techniques. It then discusses solutions available through Cisco®.

How Are Botnets Created?

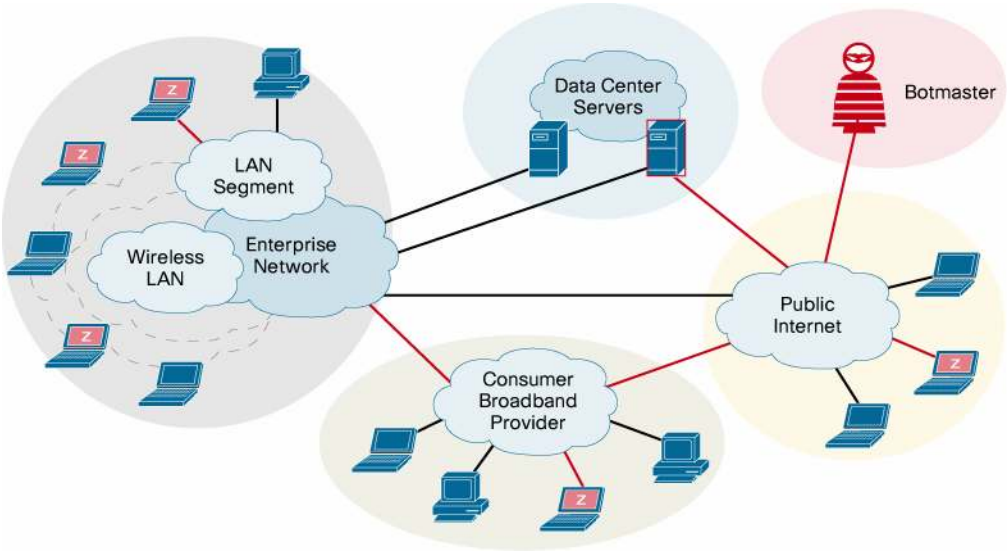
Botnet creation begins with the download of a software program called a “bot” (for example, IRCBot, SGBot, or AgoBot) along with an embedded exploit (or payload) by an unsuspecting user, who might click an infected e-mail attachment or download infected files or freeware from peer-to-peer (P2P) networks 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.

Figure 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.

The Impact of Botnets

Botnet-led exploits can take many forms.

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.

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.

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.

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.

E-Mail Spam

Most of today's e-mail spam is sent by botnet zombies. An IronPort study in June 2006 estimated that 80 percent of all spam came from zombies, an increase of 30 percent year-over-year for the same period.

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).

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.

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, such as Cisco® NetFlow. 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 technique are not always scalable.

The most common detection and mitigation techniques include:

- **Flow data monitoring:** This technique uses flow-based protocols to get summary network and transport-layer information from network devices. Cisco NetFlow 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.
- **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.

- **DNS log analysis:** Botnets often rely on free DNS hosting services to point a subdomain 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 subdomains 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.
- **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.

Cisco Products and Solutions

Cisco offers numerous products that help detect botnet proliferation and attacks, and can shut down botnets. These products are described below.

Cisco Guard Appliances and Traffic Anomaly Detectors

Cisco Guard DDoS Mitigation Appliances offer the industry’s most complete and powerful solution for detecting and defeating one of the most significant threats from botnets today: DDoS attacks. Cisco Guard appliances are based on a unique multiverification process architecture and work in concert with Cisco Traffic Anomaly Detectors, employing the most advanced anomaly recognition, source verification, and antispoofing technologies to identify and block individual attack flows in real time while allowing legitimate transactions to pass. This helps ensure availability and business continuity even while the network is under attack.

The Cisco Guard XT 5650 delivers multigigabit performance to protect the largest enterprises and service providers from distributed DDoS attacks by performing per-flow-level attack analysis, identification, and mitigation to block specific attack traffic. For more information, please visit http://www.cisco.com/en/US/products/ps5888/index.html.

Cisco IronPort

The Cisco Ironport S-Series offers an integrated Layer 4 Traffic Monitor that scans all ports at wire speed, detecting and blocking spyware “phone-home” activity. By tracking all 65,535 network ports, the IronPort Layer 4 Traffic Monitor effectively stops malware that attempts to bypass Port 80 and also prevents rogue P2P- and IRC-related activity. This enables companies to identify and remediate malware-infected systems that are attempting to connect outbound to participate in command and control networks, transmit confidential data, etc. It looks for outbound activity from the protected networks to hostile external networks.

An additional layer of protection is offered through IronPort Web Reputation Filters. These filters are based on IronPort’s SenderBase Network, the world’s first and largest e-mail and Web traffic monitoring system that collects data from more than 100,000 networks around the world. By tracking a broad set of more than 40 Web-related parameters, SenderBase supports very accurate

conclusions about any URL. If a site becomes compromised and suddenly starts distributing malicious code, this behavior lowers the site's score, causing the site to receive scanning by the IronPort Anti-Malware System.

The breadth and depth of SenderBase data allows IronPort Web Reputation Filters to stop both known and emerging threats, resulting in a malware catch rate significantly higher than signature-based Web security solutions. These techniques prevent downloads of malicious bot code and exploits, such as adware, Trojans, system monitors, keyloggers, tracking cookies, browser hijackers, and phishing. For more information, please visit www.ironport.com.

Cisco Security Agent

Cisco Security Agent defends servers, desktops, and point-of-service computing systems from the most common botnet-based attacks: installing bot code and exploits, spyware, rootkits, and targeted and day-zero attacks. Cisco Security Agent offers proactive protection against threats never seen before and new exploits and variants that try to take advantage of published and unpublished vulnerabilities of the system.

Cisco Security Agent provides visibility and reporting on host processes that communicate outside the corporate network. It globally correlates threat information and applies dynamic mitigation. It also detects anomalous activity, such as SYN floods, and can influence security policies on the network. It does this by communicating the offending host information (zombies leading an attack) with Cisco network intrusion prevention systems (deployed inline), which then shuts down access for those hosts. Cisco Security Agent can also monitor access to key files, applications, and servers from unathorized hosts. For more information, please visit http://www.cisco.com/go/csa.

Cisco Intrusion Prevention Systems

Cisco IPS sensors emply powerful anomaly detection algorithms to detect and block botnet attacks. The underlying assumption is that fast-spreading network worms and scans initiated by botnet zombies will change the overall traffic patterns in the network (for instance, from their scanning for more vulnerable hosts).

Cisco IPS sensors offer anomaly detection in two modes: a learning mode and a detection mode. In the learning mode, the sensors observe the normal behavior of your network and build a set of profiles for each network service in a histogram. In the detection mode, the sensors look for deviations from the normal profiles, and flag such behavior. The sensors watch for events such as:

- TCP SYN not followed by a SYN-ACK reply
- UDP packets not being answered with returned UDP packets
- ICMP or other protocol requests with no replies

While some failed connections are normal, Cisco IPS sensors look for deviations and then examine the patterns, classifying deviant behavior as scanner or a worm behavior. The sensors then respond with actions such as "Deny Attacker" or "Produce Alert". Using this behavioral approach, fast-spreading worms can be detected immediately, even without an up-to-date signature set. When Cisco IPS sensors are used in conjunction with Cisco Security Agent, the result is an even more powerful day-zero solution to detect and mitigate botnet attacks.

Cisco NetFlow and Cisco Security MARS

Cisco NetFlow, the industry-leading implementation of flow-based protocols, is a form of streaming telemetry that is exported from Cisco IOS® Software-based routers and Layer 3 switches. Because

of its scalabiliy and suitability for reporting information about traffic on networks of all sizes, Cisco NetFlow has become the standard method for obtaining useful information for traffic engineering and operational security for both enterprise and service provider networks. Cisco NetFlow telemetry can be used to detect botnets and perform forensics and auditing functions.

Once NetFlow is enabled on a particular network device; its telemetry data can be either viewed at the CLI, or sent to collection and analysis tools such as Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS). For more information, visit http://www.cisco.com/go/netflow.

Cisco Global Site Selector

Cisco Global Site Selector is a global load balancer that can also serve as a DNS server to provide scalable naming and addressing services for enterprise and service provider networks. As either a load balancer or DNS server, it can mitigate the effects of a DNS-based DDoS attack. This distinctive self-protection capability can be deployed to shield any DNS infrastructure, including Berkeley Internet Name Domain (BIND) services, Microsoft-based client devices, and Microsoft Active Directory.

Cisco Global Site Selector uses a subset of the unique multiverification process architecture found in Cisco Guard DDoS Mitigation Appliances. The Global Site Selector continues to process legitimate DNS traffic while blocking the attack traffic. Its features include rate-limiting, filtering, and spoofing prevention. For more information, please visit http://www.cisco.com/go/gss.

Table 1 compares these Cisco solutions.

Table 1. Threat and Cisco Solution Matrix

Cisco Technology	Types of Botnet Threats			
	DDoS Attack	Spyware, Malware, Adware	Phishing	E-Mail Spam
Cisco Guard Appliances and Traffic Anomaly Detectors	Detect and prevent attack	–	–	–
Cisco NetFlow and Cisco Security MARS	Detect attack	–	–	Detect attack
IronPort S-Series	–	Prevent Infection	Prevent attack	Detect and prevent attack
Cisco Security Agent	Detect and mitigate attack	Detect attack and prevent infection and damage	Detect attack and prevent damage	Detect attack and prevent damage
Cisco IPS Sensors	Detect and prevent attack	Detect attack and prevent infection	–	–
Cisco Global Site Selector	Detect and prevent attack	–	–	–

Conclusion

Botnets have emerged as one of the most significant security threats on the Internet today. Due to the multiple infection and attack vectors they use, no single security technology can defend against all botnet threats. Cisco provides the most comprehensive suite of products in the security industry to defend against botnets. For more information, please visit http://www.cisco.com/go/tcc.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-448516-00 12/07

