Anatomy of a Botnet

Abstract/Introduction:
One of the greatest challenges in Internet security today is how to contain the global scourge that is the botnet. Botnet authors and their criminal organizations are continuously developing innovative ways to recruit new victims into their networks and monetize them.

Part of the difficulty in combating botnets is the lack of understanding around the following questions:

- Who are the people behind them?
- Why are they so prevalent, and what motives are behind their use?
- How do attackers create and deploy a botnet infrastructure?
- How to determine if a system is already part of a botnet?

This paper will answer those questions, as well as what is being done to combat them today.

What Is a Botnet and How do Cybercriminals Use It?
In its most basic form, a botnet is a group of computers that have been infected with malware that allows its controller (or ‘master’) to take some measure of control over the infected machine. Each botnet – and there are likely thousands of them operating today – is used by its master to perform a range of unsavory activities without the knowledge of the victim. Once infected with botnet malware, the computer becomes a mindless zombie – ready to do the bidding of its master.
Cybercriminals use botnets to generate revenue in many different ways:

- **Distributed Denial of Service (DDoS) attacks**: The intent of a DDoS attack is to direct so much traffic at a web server that it becomes overwhelmed and cannot respond to legitimate requests. A common technique is to launch a very brief attack to extort ‘protection’ in exchange for not launching another more widespread attack (Sites that are event-specific, such as online sportsbook, are particularly vulnerable to the threat of being knocked offline during a major event like the Super Bowl or World Cup).

- **Spamming**: The first botnets existed primarily to send spam, and to this day, spamming is still one of the biggest activities botnets perform. Infected machines will act as email relays for the bot master and can send out staggering numbers of unsolicited emails per day. Some of the largest botnets in history were responsible for sending out literally billions of messages a day.

- **Financial fraud**: Botnets in recent years have expanded the scope of their operations into banking fraud. With the ability to install additional malware onto an infected machine, bot masters can siphon off valuable information such as a social security or credit card number, a name, address, date of birth and any other information that enables them to quickly and efficiently take money from bank accounts or credit cards.

- **Search Engine Optimization (SEO) poisoning**: Botmasters boost search engine rankings artificially to drive searchers to Websites that inject malware into a victim's machine, or send the victim to sites that sell counterfeit goods or fake prescription drugs.

- **Pay-per-Click (PPC) fraud**: A bot master will set up a legitimate-looking website and recruit legitimate advertisers. The website owner’s botnet, working in the background, will visit the site and click on ads. The advertiser then pays the owner of the botnet for the botnet-generated activity, as the clicks are coming from thousands of different machines from geographically unique locations.

- **Corporate and Industrial Espionage**: While experts in cybercrime fiercely debate the true scale and scope of using a botnet to perform espionage, there is evidence that some botnets have been used in combination with targeted email attacks against both corporations and governments in the attempt to steal valuable intellectual property information and state secrets.

- **Bitcoin Mining**: Bitcoin is a virtual currency that can be traded anonymously online for products and services. Bitcoins are “mined” by installing a program on a user’s PC that performs complex calculations; the user is then rewarded with a bitcoin for their efforts. By installing bitcoin software on a victim’s PC, a bot master can harness the processing power of that computer to mine coins and sell them on the grey or black market for real currency.

### How a Botnet Works

The methods of infecting a user’s computer with a bot are almost as varied as the ways in which cybercriminals use botnets.

- **Drive-by Download**: Simply visiting a malicious site with a PC that hasn’t been kept current with security patches and antivirus can download and execute malware on the user’s PC, thus adding to that botnet’s ranks.

- **Email**: A more traditional yet still popular method of botnet infection is through a user opening email with malicious content, often sent by someone the user knows and trusts (whose system is likely infected with a botnet).

- **Pirated software**: Malware developers often hide malicious code inside a software download, which then installs itself on a victim’s machine when the user opens the executable.

### What Happens After Infection

During a bot’s installation, the malware typically installs what is known as a backdoor, or a program that allows the bot master to communicate, control and install software onto the infected computer. Once installed, it’s extremely difficult to shut and lock the backdoor, even after the infected computer has downloaded the newest security or antimalware updates.

After a bot has installed itself, it usually makes an attempt to communicate with its owner to check in. An infected computer can send a wealth of information back to the bot master including the infected computer’s IP address (which helps the bot master determine where the victim is located in the world), the computer’s login name, operating system, what patches have been implemented and much more.

After the bot has made contact with its master, any number of activities can occur: The master can send a newer version of the malware to install and run or tell the bot to watch
for certain patterns such as any attempts made to log into an online bank account. The botnet can also execute other commands, such as recording online activities, sending spam emails, participating in denial of service attacks, and installing additional malware on the compromised system. Competition between botnet owners is getting so fierce today that the code writers are actually writing applications that can search if a particular PC has been infected with a competing botnet and then uninstall it from the user’s system.

How a Botnet Avoids Detection

A common misconception among IT staff is that since a bot has to connect with an external Command and Control (C&C) server to be successful, existing network security tools such as IPS or antimalware should be able to block the connection. Botnets use a range of techniques to evade existing methods of detecting and blocking access to a master’s C&C server, such as maintaining a list of IP addresses with which to connect. If the first one doesn’t respond, the bot will keep going down the list until it finds an active C&C server. More advanced botnets use Domain Generation Algorithms (DGA) and fast flux to ensure the bot is always able to communicate with its C&C server:

► DGA is a method whereby the malware generates the C&C server addresses. Using a proprietary algorithm, the malware can determine when to connect to what appears to be a random address online. All a bot master needs to do is ensure they have registered that random domain name a day or two ahead of the connection time and created the appropriate DNS records to point that address to their C&C server.

► Fast flux is a somewhat different in its implementation, but the general idea is similar: Through modified DNS records, the bot master points many IP addresses to the domain names the bot attempts to contact. By changing those records regularly, the bot master ensures they can stay a step ahead of any potential actions to shut down the C&C server. Bot masters often incorporate both of these methods into their botnets in the hopes that their zombies will find some way to call home.

Stealing Your Information

Launching a denial-of-service attack, relaying spam and poisoning search engines are only part of a bot master’s bag of tricks. A bot master can also install malware on a machine that has the sole purpose of harvesting personal information, online banking credentials, or corporate secrets.

One such type of malware is called a keylogger. A keylogger monitors and records every keyboard action and then sends that data back to the bot master in specific intervals. This is one way a bot master is able to determine a victim’s user name and real name, password, date of birth, Social Security Number, email account info, bank account numbers, mother’s maiden name, telephone numbers and so on.

Two-factor authentication

One way that banks and other organizations that enable remote access to sensitive or regulated data combat data-harvesting software today is through two-factor authentication, utilizing something you know and something you have as the two factors:

► The first factor, something you know, consists of a standard login name and password.

► The second factor, something you have, consists of a unique, frequently changed password that is generated through a device such as a key fob (also known as a hardware token) or a mobile phone.

However, botnet authors have created a work-around to this approach with a Man-in-the-Browser (MitB) attack. In a MitB attack, the malware spoofs the bank’s Website and appears indistinguishable from the legitimate banking site. From the spoofed site, the user provides the information that is required for a secure login, including the unique password generated from the two-factor authentication process. When the victim enters their login credentials, the spoofed site forwards that information to the bank’s real Website, where a bot master then has access to that victim’s bank account.

Another type of MitB attack surreptitiously injects additional fields into the bank’s login page through the browser being used by the victim. These extra fields ask for more information during the login process than normal, such as mother’s maiden name and city of birth. With these details in hand, a bot master could then call the bank directly and give them those personal details, which would give them access the victim’s account.

Thankfully, banks today have sophisticated algorithms in place to help identify fraudulent activity within an account. When this happens, the bank often calls the victim to verify suspect activity. However, if the bot master has used the MitB method described above, they have most likely updated
the victim’s personal information with a phone number that points to a disposable VoIP number that goes right to the bot master. When the bank calls what it thinks is the victim’s number, the bot master picks up, verifies all of the personal information on the account and then verifies the overseas wire transfer they initiated out of the account.

Another often unreported function of botnets is the theft of confidential information and intellectual property. There are botnets in the wild today that deliver very targeted emails to corporate and government targets in the hope of installing a backdoor onto a specific user’s system (or small group of users, such as employees of the White House). Once a corporate network has been penetrated with this spear-phishing attack, the bot master will quietly search through both the victim’s computer and any shared network drives to find technical drawings, source code, bid proposals, customer lists, internal emails, and so forth.

How to Determine an Infection has Occurred

While there is no fool-proof method for determining the presence of a bot, typical symptoms can include:

- System running slower than usual
- Hard drive LED is flashing wildly even though it’s in idle mode
- Files and folders have suddenly disappeared or have been changed in some fashion
- A friend or colleague has informed the user that they have received a spam email from their email account
- A firewall on the computer informs the user that a program on the PC is trying to connect to the Internet
- A launch icon from a program downloaded from the Internet suddenly disappears
- More error messages than usual are popping up
- An online bank is suddenly asking for personal information it’s never required before

The Best Defense

Knowing how a botnet works is a good first step in defending a system from a botnet attack. Beyond education, one of the single most important things a user can do to protect themselves is to make sure all of the software they use is obtained from a legitimate and trusted source and that all applications are fully patched with the most current updates. Surfing the Internet using an outdated Internet browser or using browser add-ons such as Adobe Flash or Oracle’s Java that aren’t kept up-to-date, is asking for trouble every time the system connects to the Internet.

Other tips to prevent a botnet infection include:

- Installing an antivirus software package and keeping it up to date. Many companies provide free versions that are just as feature rich as those sold by the more known antivirus companies
- Get in the habit of setting up regular complete system scans
- Stick to one antivirus program, as running more than one can cause system irregularities
- Use a personal firewall program, and enable alerting whenever a program attempts to connect to the Internet

Show Me the Money!

The reason software developers are creating such sophisticated malware is the ability to monetize botnets while the risk involved in creating and maintaining it is quite low. This is due to the global nature of the Internet and the ways bot masters hide their location, making it very difficult to identify a bot master, let alone arrest and prosecute them.

A bot master can make thousands of dollars a day “renting out” the denial of services capabilities of their botnet to anyone with a credit card and a grudge who wants to take a particular Website offline. Bot masters have even figured out ways to segregate their botnets into smaller units, allowing them to launch multiple attacks against multiple sites. A small Website may only need a few hundred zombies attacking it to take it offline; a larger site may need thousands. By customizing the size of the attack, a bot master can maximize financial gain. A study by Kaspersky Labs estimated that in 2008, botnet owners earned about twenty million dollars just from launching DDoS attacks.

Selling personal information harvested from victims can be lucrative as well. A single account, depending on where the account is based, can sell for anywhere from $5 to $15. These accounts are typically bundled into large packages and sold to other criminals who wish to commit various methods of financial fraud or identity theft.
Spammers are also interested in buying bulk lists of email addresses collected by botnets, and will pay anywhere from $20 to $100 for a million email addresses. Botnet owners also sell the spam themselves: Current estimates are that the cost of sending 20,000 emails is about $40. The fact that some botnets are sending literally tens of millions of spam emails a day, shows just how much money they can generate. SEO poisoning can cost up to $80 for 20,000 spammed links, posts or comments.

Pay-per-Click fraud is yet another money-making opportunity. A study by Microsoft Research estimates that a full one-quarter of all online ad clicks are fraudulent. Click Forensics estimates that about 17% of ad clicks are fraudulent, approximately one-third of which are directly attributed to botnets. Based on the amount of money being spent for online advertising, click fraud may be netting bot owners tens of millions of dollars annually.

Bitcoin mining is yet another easy way for bot masters to continually create additional revenue. By installing illicit software that continually mints and transfers Bitcoins, a bot master can ensure his group of zombies is always generating money.

These monetization opportunities are not mutually exclusive—a prolific botnet operator will utilize an infected machine in most (if not all) of the methods mentioned above.

The Very Low Cost of Starting a Botnet

Botnets used to be the domain of a very small, very skilled group of criminals. Today, getting a botnet up and running costs next to nothing. For example, in May of 2011, the source code of the infamous Zeus botnet was leaked online. Anyone willing to spend some time digging around in the dark recesses of the Internet can find a copy of the software and modify it to create their own botnet. And, in December 2012, Symantec discovered an enterprising criminal selling a complete Zeus installation for those not very technically skilled for $250.

More professional botnet services can cost thousands of dollars per month to operate, but these specialized installations often include ready access to a network of infected computers and around-the-clock technical support. If an aspiring botmaster doesn’t have the programming skills to setup and deploy his own botnet, there are a wide variety of crime services that exist today that are more than willing to facilitate entrepreneurial aspirations. For example, consulting services to assist in setting up a botnet range from $350-$400.

Once built, the botnet software will need to be distributed to unwitting computers to become a full-blown botnet. There are affiliate networks known as Pay per Install (PPI) networks that exist to infect computers online and create a botnet from the ground up. These networks require only the number of infected systems wanted and the botnet software, and the affiliate network will take care of the rest.

The Minds Behind the Malware

The days of the stereotypical suburban teenage hacker causing mischief online from his parent’s basement are well behind us; today’s cyber crime organizations are run as efficiently as most legit businesses. As reported in FortiGuard’s 2013 Crimeware report, these criminal organizations have familiar hierarchical structures: executives (the guys at the top of the food chain who call all the shots and take the lion’s share of the proceeds); middle management (recruited by the executives who are responsible for carrying out infection campaigns) and the “infantry;” money mules used to help move funds. The free FortiGuard 2013 Cybercrime Report can be downloaded here: http://www.fortinet.com/resource_center/whitepapers/cybercrime_report_on_botnets_network_security_strategies.html

While most botnet organizations are set up in Eastern Europe and Russia due to the ease with which bot masters can move money and avoid prosecution, there have also been botnets based out of China, Thailand, the UK, South America and in the USA, illustrating that bot masters are truly a global scourge.

Botnet authors do more than rest on their laurels and rake in money once they have created their networks—they are technically competent programmers who are always looking to improve upon their creations by making them harder to detect and remove, or finding new ways to monetize their infected networks. Using tactics such as hiding their command servers behind multiple layers of proxy servers, encrypting their communications or by even doing away entirely with the traditional client-server method and moving to a completely peer-to-peer structure, they continue the game of cat and mouse with antimalware and threat researchers.
Again, the cost is nominal--typical PPI networks charge around $100 per 1000 installations. Infections in areas such as North America, the European Union and Australia however typically command a premium price over infections in Asia and Eastern Europe.

For the truly ‘hands-off’ criminal business owner (or for those who find managing a botnet is simply too much work), one can rent a botnet for criminal activity. Typical costs associated with botnet rental include $535 for 5 hours per day of DDoS attacks per week, $40 for 20,000 spam emails and $2 for 30 online forum and comment spam posts.

Methods to Stop Botnet Proliferation

While it appears that botnet owners have the upper hand, there are methods being used today to help take botnets down. Companies such as Microsoft have turned to the legal system for help by filing motions against botnet owners – either by filing suit against a botnet author’s online moniker or as a John Doe. Recent successes have been made in seizing control of domain registration services that have previously allowed botnet owners to generate the thousands of domain names required to keep their C&C infrastructure alive.

Technologies such as DGA also are not without flaws. If a researcher can reverse engineer the algorithms used to generate the list of servers to which the bots are going to connect, it is possible for an antibotnet organization to seize control of the botnet by registering those domain names and establishing its own C&C server. This technique is commonly known as sinkholing and can be very successful in slowing down or eradicating a botnet – especially if the botnet malware incorporates an installer and uninstaller into the malware. Sinkholing is also an effective method for researchers to study botnets, as the process can determine the rough size of a botnet, the methods with which the bots communicate with its master, and, in some cases, determine the location or identity of the owner.

Computer Emergency Response Teams (CERTs) are also helping shut down botnets. Many countries, academic institutions and companies maintain their own CERTs, and information sharing between these teams is quite common. As they share a singular goal of trying to stop cyber criminal activity, CERTs often take the lead in trying to take down botnets. It’s likely there will be even more international collaboration between both public and private groups to stop botnets, with increased pressure on domain registrars to more rapidly respond to botnet threats.

How Botnets are Evolving

Mobile devices, such as smart phones and tablets, have become ubiquitous. With that surge in devices, FortiGuard Labs has observed a similar surge in the occurrence of mobile malware. Mobile devices have become the target of choice for many of the world’s botnet authors, and it will not be long before we see the first successful attempts to monetize these devices. The result could be the rise of toll fraud, SMS premium services and ransomware as ways to generate cash.

Another interesting phenomenon FortiGuard Labs has observed in the past year is the creation of opt-in botnets, where individuals voluntarily install a botnet on their machines. Organizations such as Anonymous distribute tools to their large group of programmers and supporters in order to launch attacks against companies, governments or organizations for political purposes. Collectively, this type of opt-in recruiting is known as hacktivism and is unlikely to dissipate anytime soon due to the ease in becoming involved by people sympathetic to a specific plight.

Conclusion

From spamming Internet users to stealing money to spying on governments, the impact of the botnet on the Internet and the global economy is massive. Botnet operators are difficult to find, hard to shut down and even harder to prosecute. The anonymous nature of the Internet and the difficulty in reaching across international borders makes the risk to cybercriminals low and thus keeps the rewards very high. It will take a much greater global effort and the ability for security organizations and nations to work quickly and in collaboration in order to deal with these botnets and their creators.
Famous Botnets Through History

**2005 Torpig:** Discovered in 2005 and noted by RSA in late 2008 to be “one of the most advanced pieces of crimeware ever created.” This botnet was designed to steal the details of online bank accounts and credit cards. Researchers at the University of California, Santa Barbara were able to seize control of the botnet for ten days in 2009 and identified over 1.2 million unique IP addresses attempting to connect to its C&C server.

**2006 Virut:** Thought to be responsible for over half a million infections globally and is able to do virtually everything in a cybercriminal’s playbook: DDoS attacks, spam campaigns, financial fraud and data theft. It has been in operation since at least 2006 and recently was dealt a crippling blow by a coordinated takedown attempt by multiple organizations.

**2007 Zeus:** One of the most financially lucrative bots in history. First discovered in 2007, Zeus was designed to secretly monitor a victim’s PC and steal banking information. The FBI estimates that to date, the Zeus botnet may have stolen hundreds of millions of dollars. In 2010, it was reported the creator of Zeus was retired and gave the source code to the creator of the SpyEye botnet. In 2011, the source code to Zeus was leaked online, which has lead to an explosion of Zeus variants. Because of this, Zeus infections and botnets continue to account for a large number of global botnet installations.

**2007 Storm:** It’s unknown exactly how many computers the Storm worm botnet managed to infect, but analyses from many different firms estimate its size at anywhere from one million to a whopping 50 million infections. Storm is famous for its ability to defend itself from reverse engineering and analysis. To date, its authors are unknown and remain at large.

**2008 Conficker:** Discovered in 2008 and has multiple variants. Early versions of Conficker were simply Internet worms that were designed to update infected machines to newer versions of the worm. Storm is famous for its ability to defend itself from reverse engineering and analysis. To date, its authors are unknown and remain at large.

**2008 Grum:** The Grum botnet (also known as the Tedroo botnet) was once the largest botnet in the world and at one time was responsible for sending hundreds of billions of pharmaceutical spam emails. The botnet was shut down in July 2012.

**2008 Lethic:** At one time, Lethic was one of the most prolific spambots in existence. At its peak, the botnet had 300,000 computers under its control and was responsible for sending out tens of billions of messages per day, which accounted for a whopping eight to 10% of global spam. While the botnet was partially dismantled in January 2010 by Neustar, Inc., its owners were able to regain full control two months later. Lethic is still in business, and it’s estimated that the botnet is now sending out about 2 billion messages daily.

**2008 Mariposa:** Primarily used for cyber scams and DDoS attacks. In 2009, Spanish authorities were able to take the botnet down, which, at the time, was responsible for an estimated 13 million infections that were capable of generating at least 250,000 Euros a month in revenue for the owners. However, while the master C & C server was dismantled, the Mariposa source code has continued to spread and is still infecting enough new machines every day to land on FortiGuard Lab’s Top 10 watch list.

**2009 SpyEye:** Initially developed in late 2009 as direct competition to Zeus, and its purpose was identical to that of Zeus: financial theft. SpyEye was even clever enough to detect the presence of Zeus on a newly infected machine and erase it. When the source code to Zeus was given to the author of SpyEye in 2010, it was assumed that newer versions of SpyEye would be built into a newer and stronger piece of malware. SpyEye remains a major source of malware infections online today.

**2010 Waledac:** The Waledac botnet is primarily known for its spam generation capabilities. At its peak this botnet had almost 100,000 infected computers at its disposal that were capable of sending out 1.5 billion messages per day. In early 2010, Microsoft seized control of Waledac’s C&C servers and crippled the botnet. However, in early 2012, threat researchers discovered that the botnet was mounting a comeback. In February of this year, the spam activity coming from Waledac was so prolific that the botnet made FortiGuard Labs Top 10 list for the month.

**2011 ZeroAccess:** Known to have infected between one and two million computers, and it is estimated that the zombie network is still generating millions of dollars per year in bitcoin mining and click fraud.

**2012 Jeef:** Jeef oOriginally started out as a parasitic file infector virus back in 2007. In 2013 FortiGuard Labs detected both a spike in infections and new evidence that suggests the virus has evolved into a full-featured peer-to-peer botnet. FortiGuard Labs is currently monitoring the activity of this botnet and will share findings as they become available.
2012 Smoke: Inexpensive malware loader that allows owners to steal passwords, launch spam attacks and install ransomware. Its inexpensive price makes this botnet enticing for new cybercriminals.

Top 10 Botnets: FortiGuard February Snapshot

FortiGuard Labs monitors botnet activity on a global basis 24/7/365. Its research is based on collected malware samples and data voluntarily reported by customers running FortiGate® network security devices installed around the world. The following Top 10 list was generated on February 13, 2013 and the ranking is based on monitored activity levels at the time.

1. ZeroAccess
2. Jeefo
3. Smoke
4. Mariposa
5. Grum/Tedroo
6. Lethic
7. Torpig
8. SpyEye
9. Waledac
10. Zeus

Successful Arrests and Takedowns

Rustock: First identified in 2006, the Rustock botnet was a major spam generator, capable of sending up to 25,000 spam emails per hour from a single infected PC. In 2011 Microsoft, in coordination with US Marshalls, FireEye, Pfizer, Dutch authorities and others were successful in shutting down the Rustock botnet, generally seen as the largest source of spam at the time. Microsoft was successful in quietly petitioning the courts in the US to pounce on Rustock’s infrastructure before its owners had the chance to move its control servers elsewhere.

Bredolab: This botnet was based out of Armenia and first identified in 2009. Dutch authorities were able to seize control of over 140 servers related to the management and operation of the botnet. After the botnet was taken over, its new benevolent owners were able to redirect infected hosts to a Webpage notifying them of the infection and how to remove it. An Armenian citizen was arrested by authorities, and the author was sentenced to 4 years in prison in 2012.

Virut: First discovered in 2006, Virut amassed a zombie base of 300,000 PCs. In January 2013, Spamhaus, in collaboration with Poland’s CERT and Russia’s Group-IB, were able to sinkhole the majority of Virut’s C&C servers, which were used to launch DDoS attacks and serve billions of pieces of spam. However, while the botnet was dealt a crippling blow, some key pieces of its command infrastructure remain alive, suggesting we may see a revival of this particular botnet later in the year.

Bamital: In existence since 2009, Bamital was used primarily for click fraud and disseminating additional malware such as fake antivirus. In February 2013, Microsoft, working with Symantec, using the same court actions they used against Rustock, raided two server facilities in the United States and shut this botnet down. Bamital, according to Microsoft’s lawsuit, was a multi-million dollar operation and infected hundreds of thousands of computers. Microsoft took control of Bamital’s C&C infrastructure and is now redirecting infected computers to a page informing them of their infection and how to remove it.