The economics of botnets

Yuri Namestnikov

How botnet owners make money 4

DDoS attacks 5

Theft of confidential information 6

Phishing 7

Spam 8

Search engine spam 8

Adware and malware installation 9

Click fraud 9

Leasing and selling botnets 10

In the past ten years, botnets have evolved from small networks of a dozen PCs controlled from a single C&C (command and control center) into sophisticated distributed systems comprising millions of computers with decentralized control. Why are these enormous zombie networks created? The answer can be given in a single word: money.

A botnet, or zombie network, is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge. Zombie networks have become a source of income for entire groups of cybercriminals. The invariably low cost of maintaining a botnet and the ever diminishing degree of knowledge required to manage one are conducive to growth in popularity and, consequently, the number of botnets.

So how does one start? What does a cybercriminal in need of a botnet do? There are many possibilities, depending on the criminal's skills. Unfortunately, those who decide to set up a botnet from scratch will have no difficulty finding instructions on the Internet.

You can simply create a new zombie network. This involves infecting computers with a special program called a bot. Bots are malicious programs that unite compromised computers into botnets. If someone who wants to start a 'business' has no programming skills, there are plenty of 'bot for sale' offers on forums. Obfuscation and encryption of these programs' code can also be ordered in the same way in order to protect them from detection by antivirus tools. Another option is to steal an existing botnet.

The cybercriminal's next step is to infect user machines with bot malware. This is done by sending spam, posting messages on user forums and social network services, or via drive-by downloads. Alternatively, the bot itself can include self-replication functionality, like viruses and worms.

Various social engineering techniques are used when ordering spam mailings or posting messages on user forums and social network services in order to cause potential victims to install a bot. For example, users can be offered an interesting video to view, which requires downloading a special codec. Of course, the user won't be able to watch the video after downloading and launching the file. In fact, the user will probably not notice any changes at all, but at the same time the computer will be infected. As a result, the computer will become an obedient servant at the beck and call of the botnet owner without the user being any the wiser.

Another widely used method involves covertly downloading malware via drive-by-downloads. This method is based on taking advantage of various vulnerabilities in applications, primarily popular browsers, to download malware to the computer when the user visits an infected web page. This is done with special programs called exploits, which use vulnerabilities not only to covertly download, but also to run a malicious program without the user's knowledge. If the attack is successful, the user will not even suspect that there is something wrong with the computer. This method of distributing malicious software is particularly dangerous, since tens of thousands of people get infected when a popular web resource is compromised.

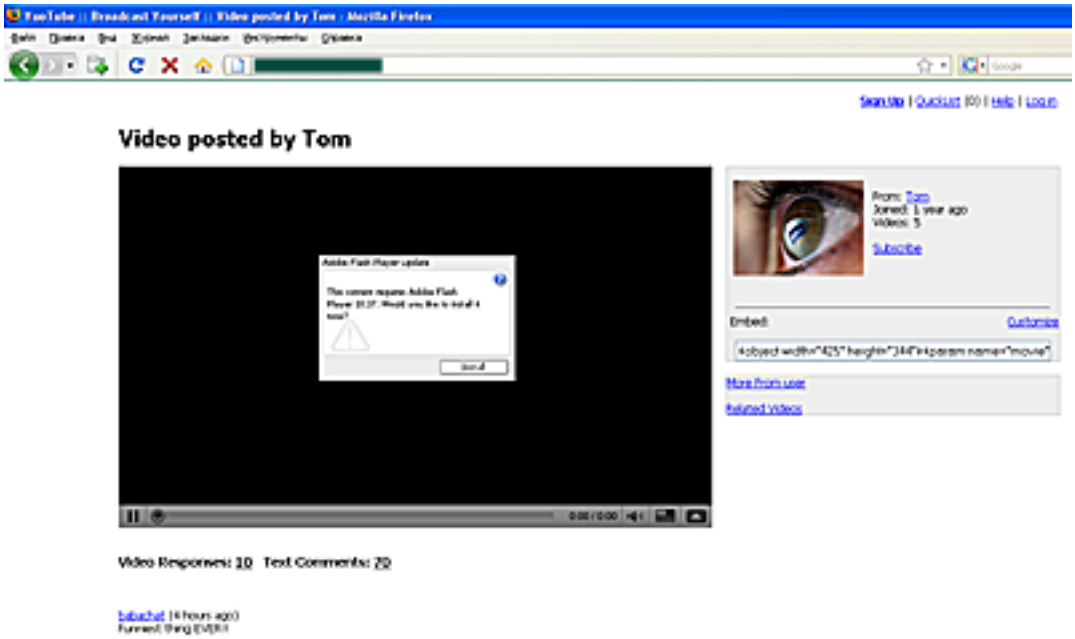

Figure1: A snare for users (a fake YouTube post)

A bot can be designed to include the feature of self-propagation in computer networks, e.g., by infecting all the executable files it can access or by scanning the network for vulnerable computers and infecting them. The Virus.Win32.Virut and Net-Worm.Win32.Kido families are examples of such bots. The former is a polymorphic file infector, the latter a network worm. It is hard to overestimate the effectiveness of this approach: today, the zombie network created by Kido is the world's largest.

The botnet owner can control unsuspecting users' infected computers via the botnet's command and control center, by connecting to bots via an IRC channel, a web connection or any other available means. It is sufficient to unite a few dozen machines into a network for the botnet to start making money for its owner. The income is directly proportional to the zombie network's stability and growth rate.

How botnet owners make money

So how do botnet owners make money with infected computers? There are several major sources of income: DDoS attacks, theft of confidential information, spam, phishing, SEO spam, click fraud and distribution of adware and malicious programs. It should be noted that, if chosen, any of these sources can provide a cybercriminal with a good income. But why choose? A botnet can perform all of these activities… at the same time!

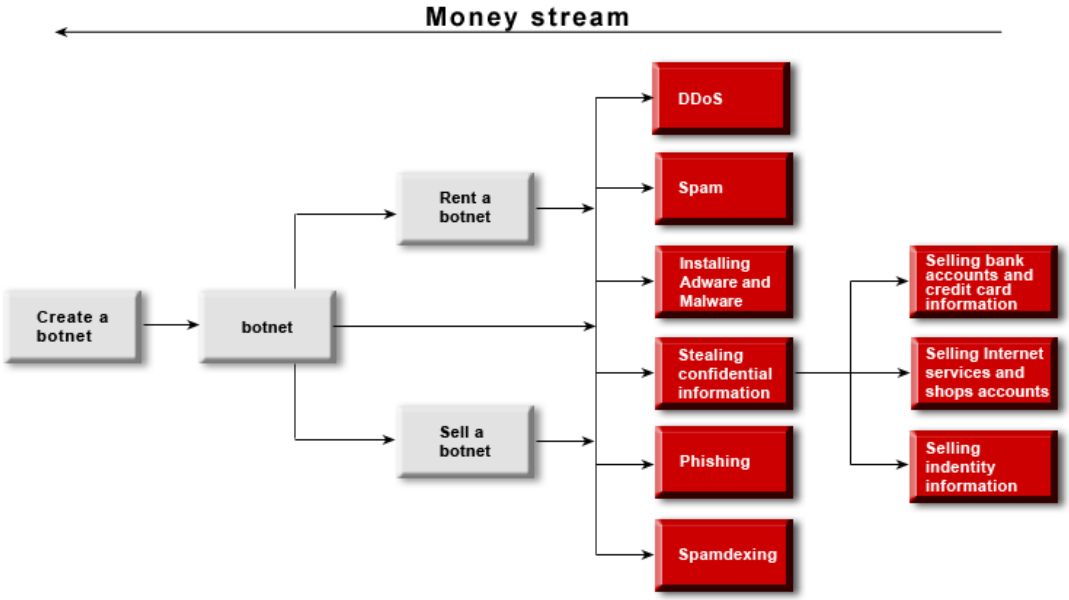

Figure 2: The 'botnet business'

DDoS attacks

Many researchers believe that even the earliest botnets provided DDoS functionality. A DDoS attack is an attack on a computer system which aims to force the system into denial of service, when it can no longer receive and process requests from legitimate users. One of the most common attack methods involves sending numerous requests to the victim computer, leading to denial of service if the computer under attack has insufficient resources to process all incoming requests. DDoS attacks are a potent weapon for hackers and botnets are an ideal tool for carrying out such attacks. DDoS attacks can be used as a tool for unfair competition or be manifestations of cyberterrorism.

A botnet owner can render services to any unscrupulous entrepreneur by organizing a DDoS attack on his competitor's website. The competitor's website will be down due to the stress caused by the attack and the cybercriminal will receive a modest (or not-so-modest) reward. Botnet owners themselves can use DDoS attacks in the same way to extort money from large companies. Companies often choose to give in to cybercriminals' demands because dealing with the consequences of successful DDoS attacks is even more expensive. In January 2009, an attack on godaddy.com, a major web hosting provider, resulted in several thousand websites hosted on the company's web servers being inaccessible for almost 24 hours. What was it, an illegal move by another popular hosting provider in the combat for a place in the sun, or was Go Daddy blackmailed by cybercriminals? We think that both scenarios are quite likely. Incidentally, the same hosting provider experienced a similar attack in November 2005, but then the service was unavailable for only an hour. The new attack was much more powerful, primarily due to the growth of botnets.

In February 2007, a series of attacks was conducted targeting the root name servers, on which the entire Internet depends for normal operation.

It is unlikely that the purpose of the attacks was to crash the Internet, since zombie networks cannot function without the Internet. It is more likely that this was a demonstration of the power and capabilities of zombie networks.

Adverts for organizing DDoS attacks are openly displayed on many user forums devoted to the relevant topics. As for the price tag, it can range from $50 to several thousand dollars for 24-hour continuous operation of a botnet carrying out a DDoS attack. The price range makes sense. The task of stopping the sales of a modest unprotected online store for one day can be tackled by a relatively small botnet (about a thousand computers), and will cost the criminal a relatively small amount of money. But if the competitor is a large international company with a well-protected website, the price will be much higher, since a successful DDoS attack will require a much larger number of zombie computers, so the customer will have to pay up.

According to shadowserver.org, about 190 000 DDoS attacks were carried out in 2008, “earning” cybercriminals about $20 million. Naturally, this estimate does not include revenues from blackmail, which are impossible to assess.

Theft of confidential information

Confidential information stored on users’ computers will always attract cybercriminals. The most valuable data includes credit card numbers, financial information and passwords to various services, such as email, ftp, IM systems etc. Today’s malicious programs allow criminals to choose the data they want by installing the relevant module on the infected computer.

Cybercriminals can either sell the information stolen or use it in their own interests. Hundreds of new bank-accounts-for-sale advertisements appear on underground forums every day. The price of an account can range from $1 to $1500. The low minimum price demonstrates that the cybercriminals involved in this business have to reduce their prices due to competition. To make a really significant amount of money, they need a steady inflow of fresh data, which is provided primarily by a stable growth of zombie networks.

Financial information is of special interest to carders, i.e., people who forge bank cards. The profitability of their operations is well illustrated by the story of a group of Brazilian cybercriminals who were arrested two years ago. They were able to withdraw $4.74 million from bank accounts using information stolen from computers.

Personal data not directly related to users’ finances are of interest to cybercriminals who forge documents, open fake bank accounts, conduct illegal transactions etc.

The cost of stolen personal data is directly dependent on the country of its legal owner’s residence. For example, a complete set of data on a US resident costs $5 to 8. EU resident data is particularly valued on the black market and is two or three times more expensive than data for US and Canadian residents. This is because cybercriminals can use this data in any EU country. Worldwide, the average cost of a full package of data on one person is about $7.

Another type of information collected by botnets is email addresses. Unlike credit card numbers and accounts, numerous email addresses can be harvested from one infected computer. The addresses harvested are then put up for sale, sometimes 'in bulk', by megabyte. Spammers are naturally the main buyers. One list of a million email addresses costs $20 to 100, while spammers charge $150 to 200 for a mailing to these same million addresses, making a clear profit.

Criminals are also interested in user accounts for various paid services and online stores. These are certainly cheaper than bank accounts, but their sale involves lower risk of prosecution by law-enforcement agencies. For example, accounts for Steam, a popular online store, with access to ten games are sold for $7 to 15 per account.

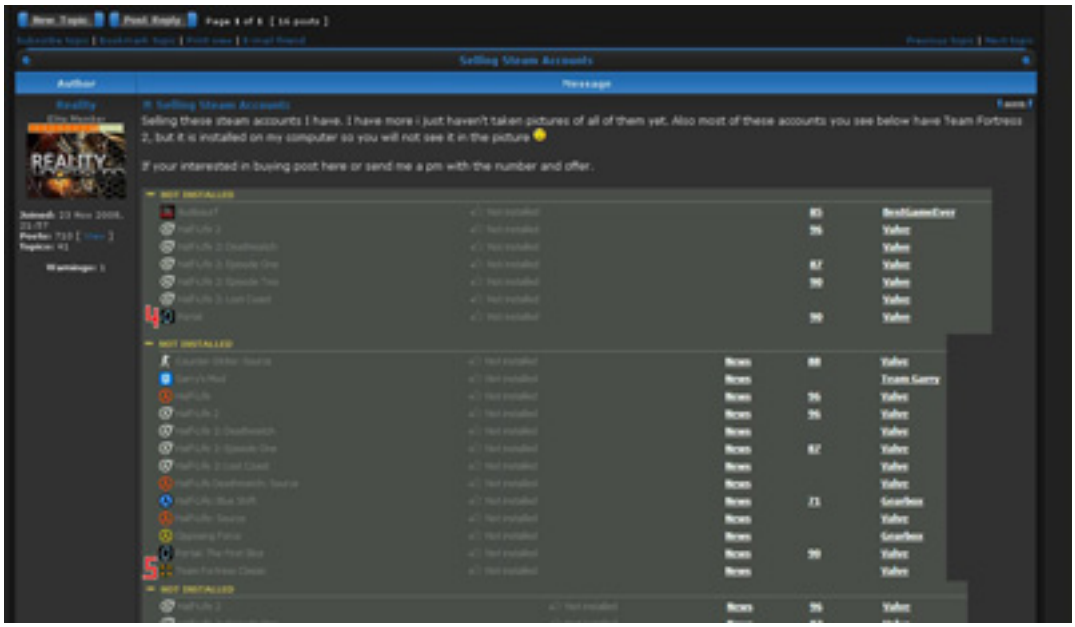

Figure 3: Forum post offering Steam accounts for sale

Phishing

New phishing sites are now mass-produced, but they need protection from closure. Zombie networks obligingly provide an implementation of fast flux technology, which allows cybercriminals to change website IP addresses every few minutes without affecting the domain name. This extends the lifetime of phishing sites, making it hard to detect them and take them offline. The idea involves using people's home computers that are part of a botnet as web servers with phishing content. Fast flux is better than proxy servers at hiding fake websites on the Web.

Thus, Rock Phish, a well-known phishing ring, works in cooperation with Asprox, a botnet operator. In the middle of last year the 'Rock Phishers', who are responsible for half the online phishing attacks and millions of dollars lost by online banking users, upgraded their infrastructure for fast-flux compatibility. This took about five months and everything was done at a highly professional level.

Instead of creating their own fast flux network, the phishers acquired a ready-made solution from the owners of the Asprox botnet.

Cybercriminals, mostly phishers, pay botnet owners $1000 to 2000 per month for hosting fast flux services.

The average income from phishing is comparable to that from the theft of confidential data using malicious programs and adds up to millions of dollars per year.

Spam

Millions of spam messages are sent globally every day. Sending unsolicited mail is a major function of today's botnets. According to Kaspersky Lab data, about 80% of all spam is sent via zombie networks.

Billions of messages with adverts for Viagra, watch replicas, online casinos etc. are sent from computers of law-abiding users. These messages clutter up communication channels and mailboxes. In this way, hackers expose innocent users' computers: the sender addresses to which mass mailings are traced are blacklisted by antivirus companies.

In recent years, the scope of spam services has broadened to include ICQ spam, spam in social network services, user forums and weblogs. This is also an 'achievement' of botnet owners: it doesn't take a lot of effort to add a new module to a bot client in order to open up new horizons for a new business with slogans such as "Spam in Facebook. Cheap".

Spam prices vary depending on the target audience and the number of target addresses. The price of a targeted mailing can range from $70 for a few thousand addresses to $1000 for tens of millions.

In the past year, spammers made about $780,000,000 sending messages. An impressive result for adverts that nobody wants, isn't it?

Search engine spam

Another application for botnets is search engine optimization (SEO). Webmasters use SEO in order to improve their websites' positions in search results, since the higher they get the more visitors will reach the site via search engines.

Search engines use a number of criteria to assess the relevance of a website. One of the main parameters is the number of links to the site located on other pages or domains. The more such links are found, the higher the search robot rates the site. The words used in the link also affect the rating. For example, the link "buy our computers" will have a greater weight for such queries as "buy a computer".

SEO is a flourishing business in itself. Many companies pay lots of money to web masters to bring their websites to top positions in search results. Botnet operators have borrowed some of their techniques and automated the search engine optimization process.

So if you see lots of links created by an unknown user or even your friend in comments on your favorite live journal entry, don't be surprised. It only means that somebody has hired the owners of a botnet to promote a web resource. A specially designed program is installed on a zombie computer and leaves comments containing links to the site being promoted on popular resources.

The average price of illegal SEO spam is about $300 per month.

Adware and malware installation

Imagine that you are reading your favorite online automobile magazine and suddenly a popup window appears, offering genuine auto accessories for sale. It would seem that there is nothing wrong with that, but you are confident that you didn't install any software to look for useful (or useless) things. It's simple: botnet owners have 'taken care' of you.

Many companies that offer online advertising services pay for each installation of their software. As a rule, this is not a lot of money – from 30 cents to $1.50 for each program installed. However, when a cybercriminal has a botnet at his disposal, he can install any software on thousands of computers with a few mouse clicks and earn serious money. J. K. Shiefer, a well-known cybercriminal who was convicted in 2007, 'earned' over $14,000 in one month using a botnet of over 250,000 machines to install adware on 10,000 computers.

Cybercriminals who distribute malicious programs often use the same approach, paying for each installation of their software. This type of cooperation between cybercriminals is called an "affiliate network". Rates for the installation of software on computers in different countries differ significantly. For example, the average price of installing a malicious program on a thousand computers in China is $3 and in the US $120. This makes sense, since computers of users in developed countries can provide cybercriminals with much more valuable information that can be used to make a lot more money.

Click fraud

Online advertising agencies that use the PPC (Pay-Per-Click) scheme pay for unique clicks on advertisements. Botnet owners can make significant amounts of money by cheating on such companies.

An example is the well-known Google AdSense network. Advertisers pay Google for clicks on their ads in the hope that users who visit their sites in this way will buy something from them.

Google, in its turn, places context-based advertising on the various websites participating in the AdSense program, paying a percentage from each click to website owners. Unfortunately, not all website owners are honest. With a zombie network, a hacker can generate thousands of unique clicks a day – one from each machine to avoid raising Google's suspicion. Thus the money spent on an advertising campaign

makes its way into the hacker's pockets. Sadly, nobody has been convicted of this kind of fraud so far.

According to Click Forensics, about 16-17% of all advertising link clicks in 2008 were fake, of which a third was generated by botnets. A simple calculation will show that botnet owners made $33 million 'for clicks'. Not bad for simple mouse clicks!

Leasing and selling botnets

Now to the busy botnet owners: for them, Marx's world-famous formula, "goods – money – goods" translates into "botnet – money – botnet". Keeping a botnet afloat, ensuring a steady inflow of new zombies, protecting bots from being detected by antivirus products and keeping the C&C from being located requires both financial and time investment from the hacker, so he simply has no time left for sending spam, installing software or stealing and selling information. It is much easier to lease the botnet out or sell it, especially since there is no shortage of those who wish to acquire it.

The lease of a mail botnet that can send about 1000 messages a minute (with 100 zombie machines working online) brings about $2000 per month. As in the case of leasing, the price of a ready-made botnet depends on the number of infected computers. Ready-made botnets are especially popular on English-speaking user forums. Small botnets of a few hundred bots cost $200-700, with an average price amounting to $0.50 per bot. Large botnets cost much more. The Shadow botnet, which was created by a 19-year-old hacker from the Netherlands and included over 100,000 computers, was put on sale for $36,000. This is enough to buy a small house in Spain, but the Brazilian cybercriminal chose the botnet.

Conclusion

Mindboggling sums make their way into the pockets of people in the botnet business. All sorts of methods are used to combat this business, but at the legislation level it is completely ineffective. Laws on spam and on the development and distribution of malicious programs or on breaking into computer networks are not applied in many countries, even where such laws do exist. Botnet owners or developers who have been prosecuted can be counted on the fingers of two hands. Which is not the case with botnets that are live on the Internet: the number of these has exceeded 3600. In fact, counting functioning botnets is not an easy task, because in addition to a few dozen large botnets that are hard to miss there are numerous smaller zombie networks that are not easy to detect or tell apart.

At present, the most effective method of combating botnets is close cooperation between antivirus experts, ISPs and law enforcement agencies. Such cooperation has already resulted in the closure of three companies: EstDomains, Atrivo and McColo. Note that the closure of McColo, whose servers hosted command and control centers for several major spam botnets, resulted in a 50% reduction in the amount of spam circulating on the Internet.

Experts follow the activity of thousands of botnets, and antivirus products detect and destroy bots across the globe, but only law enforcement agencies can stop the command and control centers and catch the cybercriminals, thereby 'putting out' botnets for extended periods of time. The closure of McColo only had a short-lived effect: several weeks later spam traffic began to go back to its usual levels. After botnet owners moved their command and control centers to other hosting providers, it was 'business as usual' for them again. What is needed is a continual effort rather than occasional inspections. Sadly, chopping off one head of the hydra is not enough!

Without help from users, combating botnets cannot be effective. It is home computers that make up the lion's share of the enormous army of bots. Neglecting to stick to simple security rules, such as using antivirus software, using strong account passwords and disabling the AutoPlay feature for removable media, can result in your computer becoming another botnet member, providing cybercriminals with your data and resources. Why help cybercriminals?