Vade Secure
Predictive Email Defense

Botnets: major players in the shadows

Author
Sébastien GOUTAL
Chief Science Officer

Table of contents

Introduction

The internet ecosystem is of an unexpected complexity, in particular its dark side. At the heart of this ecosystem, botnets occupy a key position, and are the source of a very large number of threats that keep the various information security players busy all the time.

But first of all, what is a botnet? Literally, a botnet is a contraction of two terms: “robot” and “network”. It is therefore a network of robots – “robot” referring to a computer agent or program – whose purpose is malicious. There are many examples of malicious activity; sending spam and viruses by e-mail are typical examples of botnet activity. Botnets are controlled by an actual person – the *botmaster*[(1)].

We shall present botnets to you in greater detail, by focusing on their life cycles. This perspective will allow us to understand any issue relating to botnets, as much from a technical point of view as from an economic and legal one.

(1) There can be several botmasters for a single botnet.

Birth of a botnet

The physical medium of a malicious agent, or *malware*, is a *zombie host* - this is in general a computer controlled by the botnet without the knowledge of its legitimate user. A typical example of a zombie host is a family computer positioned behind an ADSL connection, whose essential security elements are not up to date (operating system, internet browser, antivirus, etc) and which has been compromised either by the execution of an attachment containing a virus or by visiting an infected website. The advantages of exploiting such an infrastructure are undeniable from an economic point of view – expenses, whether from hardware, bandwidth or electricity, are fully taken care of by the legitimate user.

Providing the conditions conducive to the birth of a botnet amounts to creating a network of zombie hosts, through a large-scale viral infection phase. This infection phase takes place in several stages:

1. The development of a malware program that will allow the zombie host to communicate with the botnet, and carry out malicious activity. Furthermore, this development will require the exploitation of a security flaw, which may be innovative or already well known, to install the malware without the legitimate user suspecting anything. Do note that certain innovative security flaws – potentially capable of affecting even recent operating systems or software programs – can be purchased or sold on the black market.

2. The construction of an address book, which is the list of targeted users in the viral infection phase. These lists can be made up by robots that collect e-mail addresses found on the Internet [2] or even purchased directly on the black market.

3. An e-mail campaign that either contains malware in the form of attachments or references the malware via a link to the infected website. Such campaigns can even be outsourced by using the services of another botnet.

4. Receiving an e-mail containing malware in one of the forms mentioned above, and its installation by some users targeted in the viral infection phase. The infection rate can be very variable and depends on each user's level of protection and the quality of the exploited security flaw.

After this initial infection phase that allows the botnet to take on a life of its own, other infection phases may take place to broaden the botnet [3]. Botnets can reach a considerable size: for example, it is estimated that the Bredolab botnet at its peak consisted of almost 30,000,000 zombie hosts.

[2] By visiting forums for example.

[3] Likewise, infection phases can occur to rebuild a botnet that has been partially dismantled.

Life of a botnet

After malware is installed on a target host, this host will contact one of the botnet's many control and command servers[4]. These servers are used to pilot[5] the activity of zombie hosts, collect information and also update the malware: they are the cornerstone of the botnet's communication infrastructure.

The malware will spy on the target host and report any useful information: credit card numbers, passwords, personal data (first name, last name, social security number, etc for the purpose of identity theft), address books, etc. These data will then be aggregated and used directly or sold on the black market by the botmaster. It is worth noting that collected e-mail addresses are of great importance to the botnet, as they allow launching new viral infection phases that will allow the botnet to expand.

Moreover, malware programs will perform the various tasks assigned to them, some of which are:

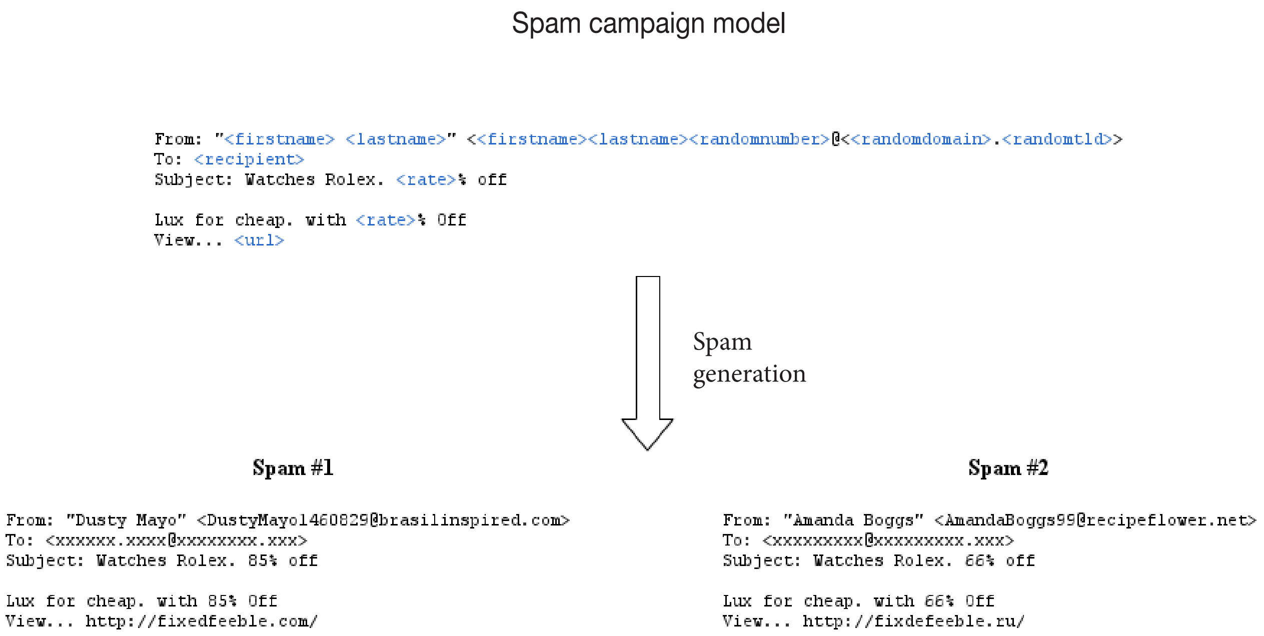
- Sending a spam or virus campaign, using an e-mail template and a list of recipients: variable and random elements will be added to this template in order to escape signature-based filter systems.
- Carrying out distributed denial of service attacks[6].
- Performing click fraud[7] to generate fraudulent advertising revenue.
- Performing intensive calculations, especially to break certain encryption keys.

[4] Control and command servers are generally installed on host sites, as they need a large capacity in terms of bandwidth, storage and processing. Piloting and monitoring millions of zombie hosts require a large amount of resources and a high level of technical expertise.

[5] Communication between zombie hosts and control and command servers is carried out according to a protocol specific to the botnet, which may possibly be encrypted.

[6] A denial of service attack consists of making an internet service unavailable by flooding it with connection requests. This is referred to as a distributed denial of service attack if a large number of machines participate in the operation, which is often the case with botnets. Some examples are the attacks launched in December 2010 by Anonymous against Paypal's, Visa's and Mastercard's websites during the Wikileaks affair, which received a lot of media attention.

[7] wClick fraud consists of automatically clicking on advertising links, challenging the economic model of sponsored links, which are highly popular on the internet. It is estimated that more than 20% of clicks on advertising links are from a fraudulent source.



Spam campaign model

```
From: "<firstname> <lastname>" <<firstname><lastname><randomnumber>@<<randomdomain>.<randomtld>>
To: <recipient>
Subject: Watches Rolex. <rate>% off

Lux for cheap. with <rate>% Off
View... <url>
```

Spam #1

```
From: "Dusty Mayo" <DustyMayo1460829@brasilinspired.com>
To: <xxxxxx.xxxx@xxxxxxxx.xxx>
Subject: Watches Rolex. 85% off

Lux for cheap. with 85% Off
View... http://fixedfeeble.com/
```

Spam #2

```
From: "Amanda Boggs" <AmandaBoggs99@recipeflower.net>
To: <xxxxxxxxx@xxxxxxxxx.xxx>
Subject: Watches Rolex. 66% off

Lux for cheap. with 66% Off
View... http://fixdefeeble.ru/
```

Example of how spam is generated from a campaign template

These activities can be carried out on behalf of a botmaster, but in most cases, they are sold as a service to other players: counterfeiters [8], organized crime rings, etc.

Take the classic example of spam:

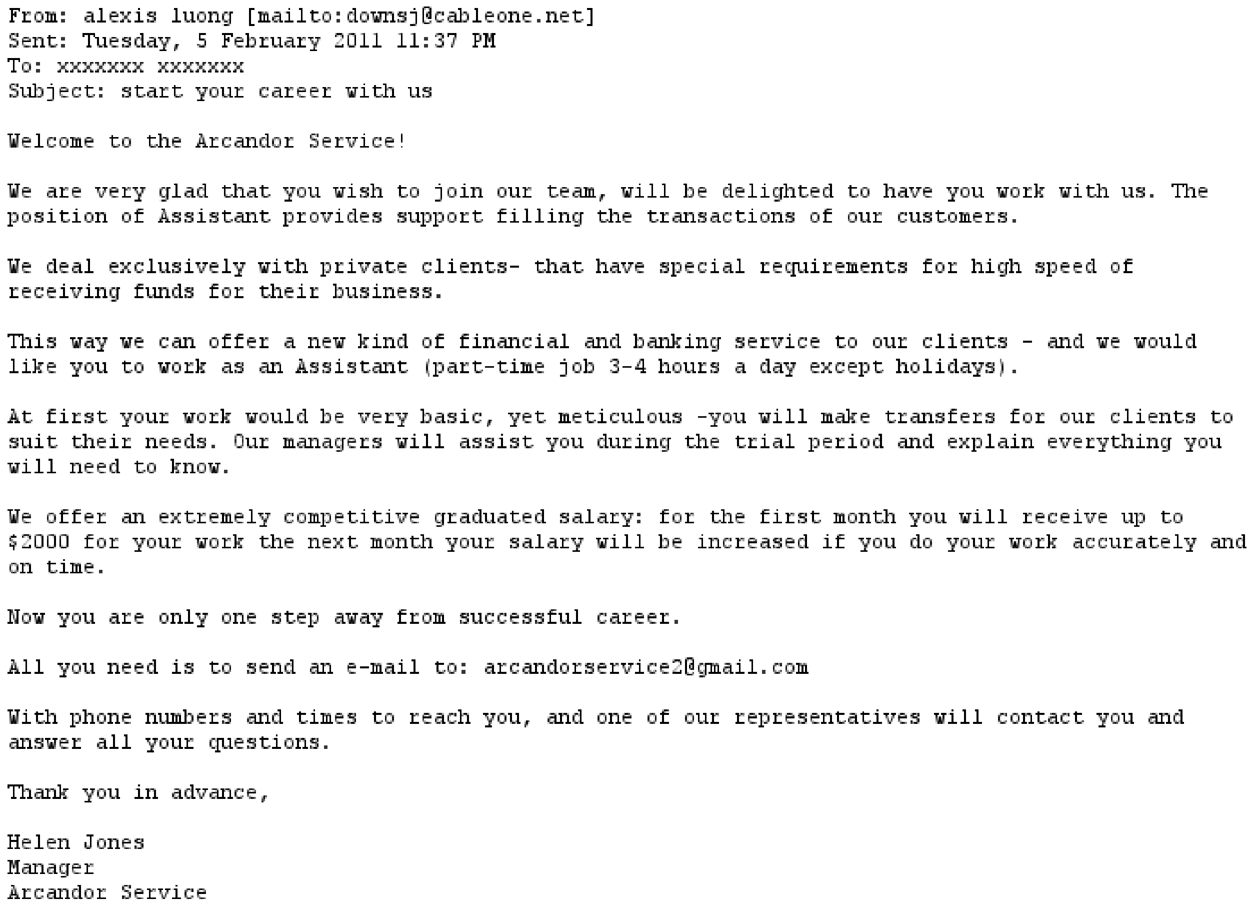
1. An organization wishes to offer the sale of counterfeit products (luxury goods, watches, etc).
2. It contacts the botmaster, and asks him to send a large-scale advertising campaign. The botmaster therefore plays the role of a service provider for mail routing: it provides – for a fee [9]- the technical resources for sending the campaign as well as the address books of recipients.
3. The spam campaign is sent, usually with a huge volume [10]. Due to the technical resources that have been implemented to fight spam, a small percentage will actually reach the intended recipient, and the transformation rate on the counterfeit site will be quite low. However, taking into account the considerable upstream volume – often several million or even billion e-mails, with practically nonexistent cost in terms of infrastructure since the financial cost being picked up by the owners of the zombie hosts – this model remains very profitable.

[8] Counterfeits mainly involve branded watches, luxury products, drugs – including Viagra – and software.

[9] Prices may vary and depend most of all on the quality of the address book. It is estimated that it costs the client on average less than $100 for sending a million spam messages.

[10] For example, the daily sending capacity of the Rustock botnet was estimated at 30,000,000,000 e-mails. This is a considerable volume, and gives an idea of how dangerous botnets are.

4. The organization that sells counterfeits then receives a large number of orders, which it can choose whether to honor: if it honors an order, it will then send the counterfeit to the client and thereby create a classic commercial relationship. If it does not honor the order, it will use the captured bank details for other purposes.
5. Since the money that the organization has earned from selling counterfeits remains illegal, it will need to be laundered. As such, it can use the services offered by the botmaster again by sending an e-mail campaign to recruit *money mules* [11]. A money mule is a physical person who accepts – for a large amount of money – to carry out banking operations on behalf of a company. These banking operations allow the company to launder large sums of money, and unknown to the money mule, he bears all of the legal liability relating to this operation.



```
From: alexis luong [mailto:downsj@cableone.net]
Sent: Tuesday, 5 February 2011 11:37 PM
To: xxxxxxx xxxxxxx
Subject: start your career with us

Welcome to the Arcandor Service!

We are very glad that you wish to join our team, will be delighted to have you work with us. The
position of Assistant provides support filling the transactions of our customers.

We deal exclusively with private clients- that have special requirements for high speed of
receiving funds for their business.

This way we can offer a new kind of financial and banking service to our clients - and we would
like you to work as an Assistant (part-time job 3-4 hours a day except holidays).

At first your work would be very basic, yet meticulous -you will make transfers for our clients to
suit their needs. Our managers will assist you during the trial period and explain everything you
will need to know.

We offer an extremely competitive graduated salary: for the first month you will receive up to
$2000 for your work the next month your salary will be increased if you do your work accurately and
on time.

Now you are only one step away from successful career.

All you need is to send an e-mail to: arcandorservice2@gmail.com

With phone numbers and times to reach you, and one of our representatives will contact you and
answer all your questions.

Thank you in advance,

Helen Jones
Manager
Arcandor Service
```

Example of an e-mail to recruit a money mule

[11] The term *mule* refers to the informal term for a person transporting drugs from one country to another, sometimes without his knowledge.

Death of a botnet

Given the essential role given to control and command servers, the dismantling of a botnet begins by putting out these servers. Such operations require the intervention of authorities to crack down on companies that host control and command servers.

The case of the Bredolab botnet can be cited again. On October 25th 2010, it was severely weakened after Dutch authorities seized 143 servers from the Dutch hosting company LeaseWeb. Nonetheless, the botnet is still alive, thanks to the presence of other control and command servers in Russia and Kazakhstan.

Another example is the Grum botnet, which was completely dismantled in July 2012, with joint operations led by authorities in Holland, Panama and Ukraine.

The ability to put out a botnet depends mainly on the actual willingness of the authorities to cooperate in the countries where control and command servers are hosted – the problem is no longer technical but legal and political.

About Vade Secure

Vade Secure is the global leader on anti phishing, spear phishing, malware and ransomware filtering. Language independent, the filter analyzes globally all incoming emails (links, attached files, content…) to detect all threats in zero-day, even the most targeted attacks. After elimination all threats, we eliminate the nuisance of low priority emails with the Graymail Management. Ads, social networks notification and newsletters are automatically sent to the graymail folder while the Safe Unsubscribe button eliminate them forever.

Protecting more than 400 million of mailboxes in 76 countries, our solutions are used by major ISPs, OEM and Enterprises worldwide. Vade Secure is implanted in 5 countries (USA, Canada, France, Hong Kong and Japan) to offer a 24/7 support.