Inside the mind of a spammer

Unsolicited Commercial Email (UCE), usually called *Spam*, is that very well known phenomenon which litters our e-mailboxes of unsolicited, unwanted and undesired emails of 'advertisement'. The most common perception of this phenomenon is that of a nuisance, something which is really annoying but not much more. Actually those who know and fight UCE, consider it an outright but subtle crime.

In this article we will try to consider UCE not from the point of view of the recipients of the emails, but from that of the sender, the *Spammer*.

First of all, there must be a clear economical advantage for the sender to inundate our e-mailboxes with UCE messages. Indeed today it is estimated that from 75% to 95% of all emails sent in Internet are UCE messages. Being criminal organizations behind UCE, it is difficult to assess the real economical value of it since these organizations obviously do not declare to tax offices their activities. But lets make a rule-of-thumbs computation.

Suppose to send 1 million UCE messages (this is a low number) of which only 10% arrives in recipients e-mailboxes and 90% is blocked by anti-spam filters. Suppose also that of these 100,000 messages delivered only 0,1% leads to an economical transaction and that each transaction has a value of 10$ (again a low number). The total for this UCE run is then of 1,000$. Not too bad for something that can be done in the matter of a few hours.

Of course there are expenses, as we will see, and all numbers mentioned can vary quite a lot depending on the type of merchandise, purpose of the message (in some cases the purpose is just to steal your credit card data, not to sell something, or to influence your opinion about something else to

the sender interest), number and list of recipients which can be generic or belong to a carefully selected group.

In a typical UCE operation three roles can be designed, even if the same individuals can represent more than one of them, and in some cases all three.

The first role is that of the *Vendor*, that is of those who have a message to send out. The message can advertise some products, usually illegally imported or sold, cracked software etc., or is a clear fraud, like the Nigerian scam or the fake lotteries, or a trick to get your credit card or bank/financial account credentials, like the fake VISA or eBay messages. Phishing is also based on UCE messages. The Vendor is the origin of the crime, and the one who will most benefit of the financial profit at the end. In other words, the Vendor is the one who invents the fraud.

The Vendor contacts the *UCE Professional* who prepares the message and selects the list of recipients. Both these tasks are delicate and technically non trivial. Indeed the message must be crafted in such a way to escape detection by the spam-filters (of which one of the most famous and open source is SpamAssassin) which check the contents of the emails. Currently one of the preferred way is to send a text message containing garbage or a real news copied from a news agency (this to escape for example Bayesian filters) and put the UCE message in an attached and obfuscated image (so to escape also image recognition software).

The selection of the list of recipients is also very important. A generic list can cost little but the risks for the Vendor are two: the first is not to reach his potential customers but only people not interested in the product, the second that the message is very quickly intercepted by anti-spam organizations which will introduce immediately ad-hoc filters. Indeed good lists usually do not include email addresses managed by internet providers known to be very aggressive against UCE.

Finally, once prepared the message and the list of recipients, the message must be sent. The third role is that of the *UCE Deliverer*, usually a highly technical organization which has the means to send all the emails without being caught. One of the typical procedures to do that is the following. The UCE Deliverer creates a virus and distributes it to as many machines connected to internet as possible,

from hundreds to millions. Once installed on a PC this virus hides itself so that the owner and the users of the machine do not realize that it is there. The virus then awaits for orders from the UCE Deliverer. The virus does not do any harm to the PC, but uses the PC for the advantage of his remote controller: from Denial of Service (DoS) attacks to others, to sending UCE emails or being a temporary deposit of stolen or illegal material. Usually these PCs are called *Bots* or *Clones* and their networks *Botnets*.

Thus the controller of a Botnet uses the PCs of unaware people to send UCE messages: he just downloads to the Bot the message to be sent, the list of recipients and gives the order to send it to them. It is practically impossible to trace back the Botnet master, or UCE Deliverer, from the infected PC since the connection between the master and the Bots is usually done through anonymizing services. In theory the owner and the users of PCs are the persons considered responsible for what it is done with them, and they often face the difficult task of proving to the authorities that someone else is responsible for what has been done with their PCs.

There are other ways of sending UCE messages, like through broken web sites or smtp open-relays, and a message can be sent using a mixture of all existing possibilities.

Besides avoiding to be traced back, the UCE Deliverer must also avoid that his Bots are discovered and included in the anti-spam Blocking Lists. Usually email servers consult these lists (like the one of the Spamhaus project) before accepting an email message form a remote machine.

In the last months there has been a change in the quality of the Bots which makes more difficult to block them. Indeed up to 2005, most bots were sending the UCE messages directly to the recipients. Now instead the Bot software checks which email provider the rightful owner of the PC uses, and sends the messages through the same provider so that they appear to come from a trusted source. Of course it is not possible to put email servers like the ones of AOL in a Blocking List only because some of their customers have a Bot on their PC which sends UCE messages through them, so other approaches to block spam are taken (but they are not discussed here).

Having sketched how UCE messages are created and delivered, we would like now to add some

concluding remarks.

If in a very few cases it has happened that a Vendor was unaware of exactly what he was doing, the operations of the UCE Professional and Deliverer can be considered from many points of view just criminal. Indeed they aim to bypass filters and defenses of the recipients, breaking into other people machines and using them with the purpose of an economical gain in doing so. The gain of the UCE Professional and Deliverer can be sharing part of the profit of the operation or just a fixed price for their work, independent of the results and the profit of the Vendor. Indeed sometimes the Vendor can be the cheated one, having to pay the others without making a clear profit.

Why then is UCE largely just considered a nuisance and a cost in infrastructures for the Internet Providers (since 9 out of 10 email messages are UCE) ?

There is not a clear answer to this, but various factors concur to it. Those who run these operations are often very well hidden and difficult to trace. They operate in a virtual way from many remote countries and often a single operation lasts just a few days. Thus besides tracing, also legal prosecution is often almost impossible.

Moreover in many legislation it is not clear if bypassing anti-spam filters with the intention of making an economical transaction is just a commercial activity or a crime. Notice that for those who are not aware of what actually UCE is, it just looks like undesired advertisement. It could violate some privacy laws, be annoying, sometimes disturbing, but still advertisement not too different from what we see on the walls in our cities or receive in our mailbox in paper format. On the other side, if UCE would be stopped, most of the current security risks and dangers of ICT would disappear.

So UCE is often considered as a bad advertising practice more than a criminal activity, and probably for this reason it is not fought as it should be.

Andrea Pasquinucci

Senior Security Professional
PhD, CISA, CISSP