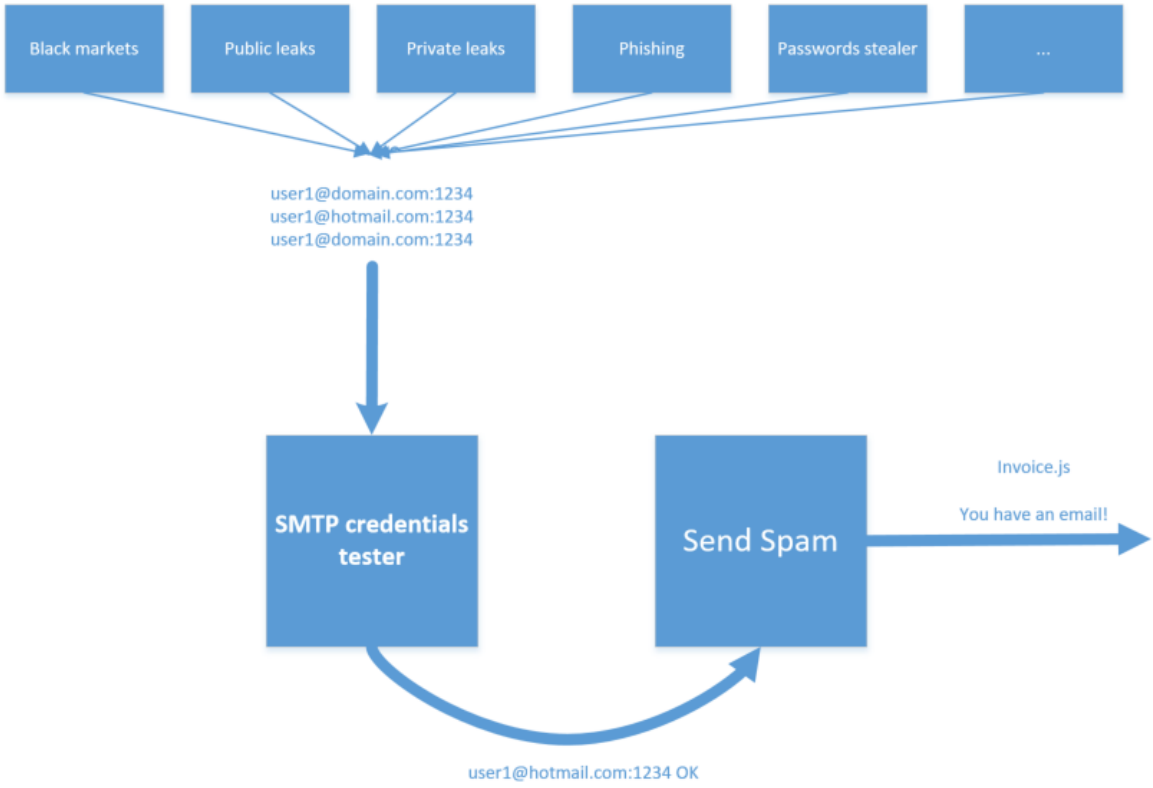
From Onliner Spambot to millions of email's lists and credentials

benkowlab.blogspot.com/2017/08/from-onliner-spambot-to-millions-of.html



Hey! It's time for another writeup about spambot. Here I will explain how I have found millions of emails and credentials on a spambot server and why your creds can be in these databases.

> Processing the largest list of data ever seen in @haveibeenpwned courtesy of a nasty spambot. I'm in there, you probably are too.
>
> — Troy Hunt (@troyhunt) 28 août 2017

I have written a lot about spambot on this blog for many reason. Spambots are often ignored by researchers and I don't understand why. In a successful cybercrime campaign there are different parts, the final payload is important but the spam process is very critical too. Some malware campaigns like Locky are successful also because the spamming process works well. This case is a good example :).

Spam the world

As introduction, we will have a look at what is a spambot, why crooks use them and why they need huge list of credentials. In the past, it used to be easier for attackers to send mass spams: they just had to scan the Internet to find vulnerable SMTP server (with weak passwords or in Open Relay mode) and use them to send Spams. However, nowadays, it's more complicated. There are a lot of anti spam companies, products or firewalls. Most of the open relays are blacklisted and the attackers have to find another way to send mass spams. Among the available options, I have seen 2 very common behaviour:

PHP Mailer

The most used tricks I have seen is to use compromised websites. For instance, this kind of spamming campaign has been used for a big Andromeda campaign. The principle is simple:

- The spammer hacks a lot (10k/20k) of websites (via well known vulnerabilities on Wordpress, Joomla, OpenCart or FTP/SSH bruteforce etc) or buy access to a lot of websites on a random shop
- He uses these websites for hosting a PHP script in charge of sending emails.
- He controls all the websites via a software or a web panel and uses them to send spam

Due to the almost infinite number of out-of-date websites on the Internet, it's difficult to blacklist every websites and it's really easy to use them for the spammer.

Malware spammer

The other common way to send spam is more brutal. Here, the attacker creates or buys a specifique malware used to infects people and send spams. The more the attacker infects people, the more he can distribute spams through different IPs. However, a random pwned Windows machine is not enought to send spam. For that, the attacker needs some email server (SMTP) credentials. This is where you can be concerned by Spambot :) Indeed, to send spam, the attacker needs a huge list of SMTP credentials. To do so, there are only two options: create it or buy it :D And it's the same as for the IPs: the more SMTP servers he can find, the more he can distribute the campaign. Lets go through an example to see how attackers create SMTP credentials lists:

Credentials: Spambots gasoline

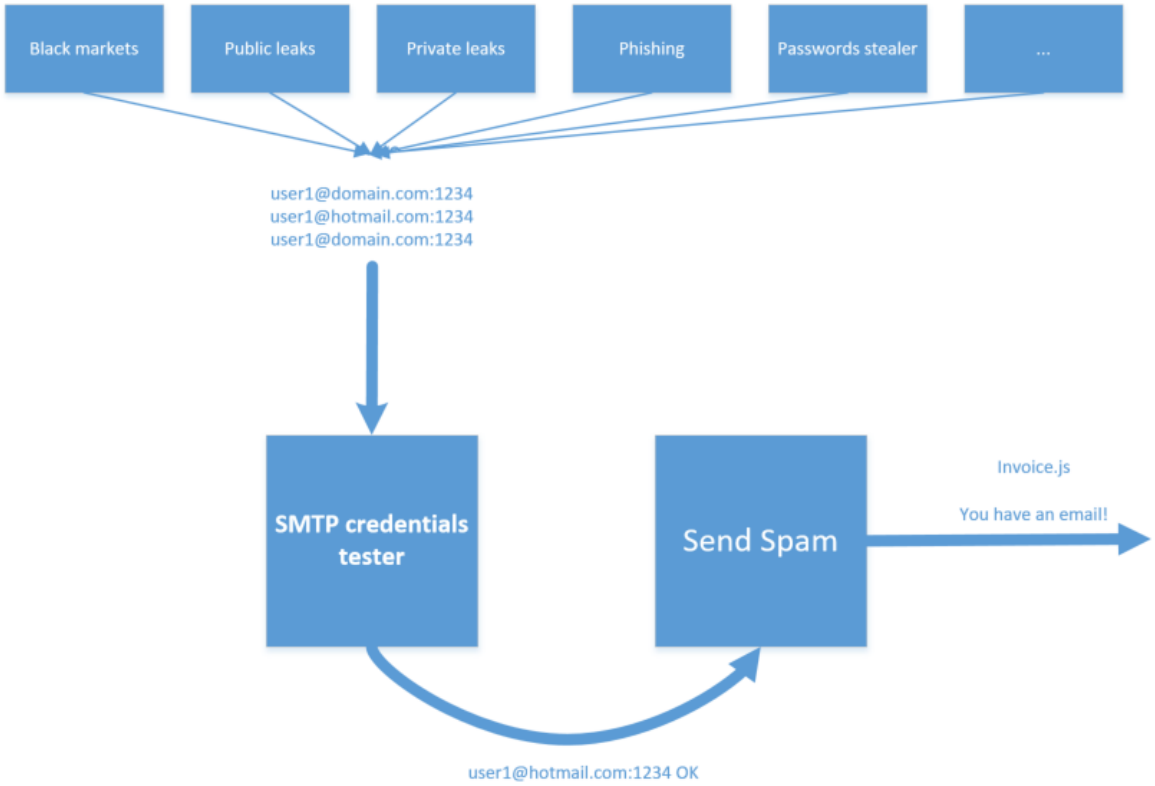
I will take as an example the Onliner spambot. This spambot is used since at least 2016 to spread a banking trojan called Gozi. I have seen this spambot targeting specific countries like Italy, or specific business like Hotels. Some emails example: DHL notification: Email targeting Hotel business: If you're curious about this case, I have tried to give some details in 3 blog posts:

- A journey inside Gozi campaign
- Spambot safari #2 - Online Mail System
- A third look at JSDropper/Gozi campaign - Proxy Statistics

TL;DR: this malware, after infecting your machine, uses 2 modules:

- A module in charge of sending spam
- A module in charge of creating a huge list of SMTP credentials

To create the list, the attacker provides to the second module a list of emails and credentials like sales@cliffordanddrew.co.uk / 123456 or peter.warner@mcswholesale.co.uk / MysuperPass. Then, the module tries to send an email using this combinaison. If it works, credential are added to the SMTP list. Else, credentials are ignored. Thanks to free email services like outlook, gmail or your ISP, the attacker can suppose that a lot of people reuse the same password and use your outlook adress to send spam :)



It's difficult to know where those lists of credentials came from. I have obviously seen a lot of public leaks (like Linkedin, Baidu or with every passwords in clear text) but credentials can also came from phishing campaigns, credentials stealer malwares like Pony, or they can also be found in a shop. Somebody even show me a spambot with a SQL injection scanner which scan Internet, looks for SQLi, retrieves SQL tables with names like "user" or "admin". Thanks to an open directory on the web server of the Onliner Spambot CNC, I was able to grab all the spamming data It's composed of ~40GB of emails, credentials or SMTP configuration. These data are composed of:

- Huge lists of credentials like email:password (in clear text)
- Huge lists of Emails to spam
- Spambot configuration files

I have found around 80 millions credentials (unsorted, it's an estimation, I cannot deal with so big txt files). One part (~2 millions) seems to come from a Facebook phishing campaign, those I have tested seems to be working and were not on HIBP. Therefore, it's difficult to say where did your credentials come from.

Making emails lists like a pro

Inside all these data, we can see a lot of emails (used for sending spam to). Because I have been following these guys for almost a year I'm able to explain how they built these lists. After looking at the spambot logs, I have seen that it was used to send fingerprinting spam. What does this mean?. Before starting a new malware campaign, the attacker used the spambot to send this kind of emails: If you look at the email you will see that inside this random spam, there is a hidden 1x1 gif. This method is well known in the marketing industry. Indeed, when you open this random spam, a request with your IP and your User-Agent will be sent to the server that hosts the gif. With these information, the spammer is able to know when you have opened the email, from where and on which device (Iphone ? Outlook?...). At the same time, the request also allows the attacker to know that the email is valid and people actually open spams :). This is an example of a classification script found on one Onliner spambot server: Example of output : As a reminder: **DON'T OPEN SPAM!**

Conclusion

If you're a malware researcher, it's time to look deeper in the spambot business. It's a creative market which interracts with a lot of other cybercrime business. Around Spambot you will often found phisher, password stealer botmaster, website scanners, malware developers, dropper developers, payload hosters, and so on. The way is maybe short between the lame Pony you have received last month in a stupid .ace archive and a spambot that spread Gozi.

Annexe

Some urls found in spam configuration files:

- hxxp://119.28.18.104/IMG_8026.zip

- hxxp://21emb.com/IMG_0557.zip
- hxxp://cielitodrive.com/2.docm
- hxxp://cielitodrive.com/IMG_0557.zip
- hxxp://dcipostdoc.com/3.docm
- hxxp://fondazioneprogenies.com/1.docm
- hxxp://fondazioneprogenies.com/IMG_7339.zip
- hxxp://intesols.com/IMG_8026.zip
- hxxp://jltl.net/IMG_8026.zip
- hxxp://liyuesheng.com/Report_Bill_ID20039421.zip
- hxxp://lopezdelaisidra.com/107490427.zip
- hxxp://maikaandfriends.com/Report_Bill_ID20593601.zip
- hxxp://mc-keishikai.com/Report_Bill_ID73086492.zip
- hxxp://pacific-centre.com/IMG_8026.zip
- hxxp://reliancemct.com/IMG_9647.zip
- hxxp://resital.net/IMG_0557.zip
- hxxp://speaklifegreetings.com/IMG_9647.zip
- hxxp://tspars.com/087578952.zip
- hxxp://usedtextilemachinerylive.com/IMG_9647.zip
- hxxp://webtoaster.net/IMG_0273.zip
- hxxp://whatisaxapta.com/5.docm
- hxxp://womenepic.com/4.docm
- hxxp://www.loidietxarri.com/Report_Bill_ID87793518.zip

Thanks to Hydraze for reviewing \o/