The mechanisms of a targeted phishing attack

Table of Contents

1. INTRODUCTION

Since the end of March, as part of our CSIRT activities, several cases of targeted phishing by email have been reported by some of our clients. This article describes in depth the mechanism of such an attack, and the measures taken by a hacker to cover his traces.

The effectiveness of the campaign will not be described in this article.

In every phishing attack, a hacker attempts to obtain sensitive information and/or money, for malicious reason, by any means of electronic (e.g. emails, instant messaging, …) and non-electronic (e.g. phone) communication.

The case study presented in this article covers, in particular, a targeted email phishing attack.

2. PHISHING ATTACK vs TARGETED PHISHING ATTACK

A typical phishing attack can be usually described as "quantity over quality", while a targeted attack will be described as "quality over quantity".

A typical phishing attack will rely on a large distribution list (also known as **mass phishing attack**), with low sophistication, in order to be executed quickly.

The larger the attack is, the faster it will be blocked by antimalware and/or antispam. As soon as the attack is blocked, the hacker will be able to run a new one, on the same distribution list or on another, introducing only minor modifications in the pattern. Generally, the income per victim is lower, but it is offset by the quantity.

On the other hand, a targeted phishing attack (also known as **spear phishing**) will need much more preparation in advance. The hacker will have to thoroughly research information about the victim, to be as convincing as possible. The incomes per victim are potentially much higher. As the distribution list is from far much limited, the campaign can last longer. By contrast, this type of attack is difficult to reuse on other distribution list because of its specific nature.

3. PHISHING SCENARIO

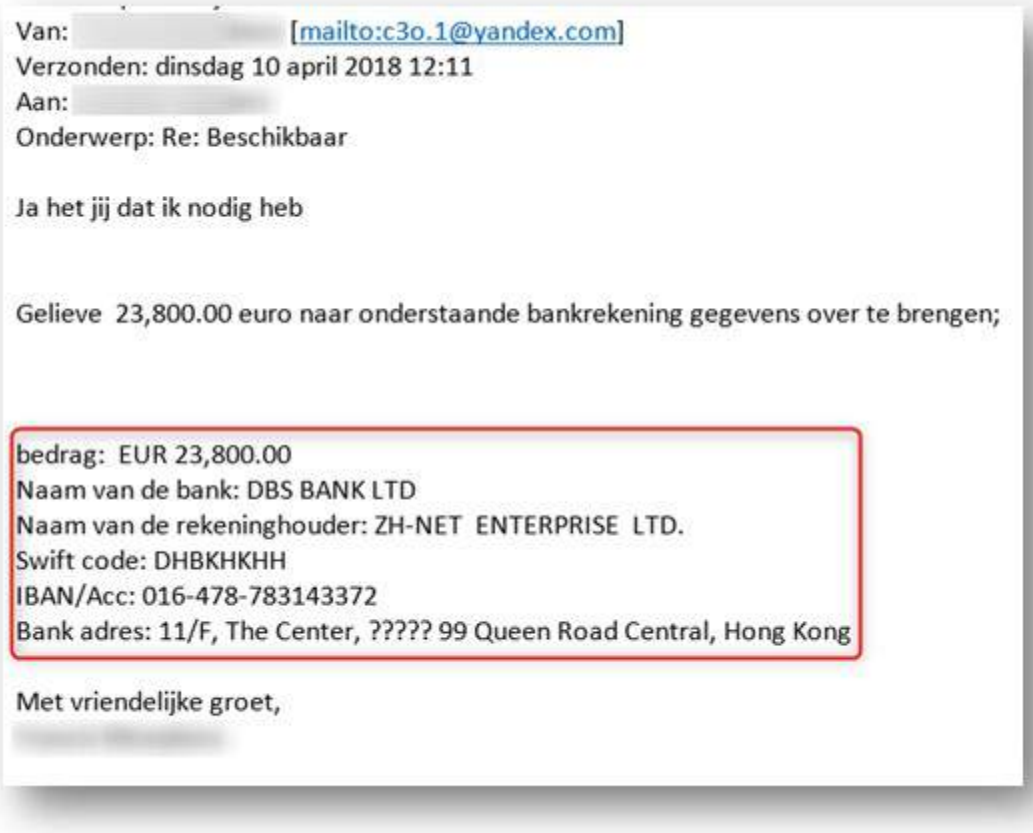
A phishing message is sent in the name of a **CEO (1) to a collaborator (2) but linked to a mailbox c3o.1@yandex.com.**

The originating email address, the subject (*"Re: Beschikbaar"* or *"Re: International overschrijving"*) and the content is about always the same (see the screenshot below).

So far, the phishing mails are sent in Dutch, targeting especially Flemish/Dutch companies.

In case of reply to the original message, a discussion starts with the hacker. In most cases, including many details, giving like more credit to the hacker.

At last, the hacker asks his victim for a payment, with a variable amount (probably depending on the size of the company), using an account in Hong Kong.



Van: [mailto:c3o.1@yandex.com]
Verzonden: dinsdag 10 april 2018 12:11
Aan:
Onderwerp: Re: Beschikbaar

Ja het jij dat ik nodig heb

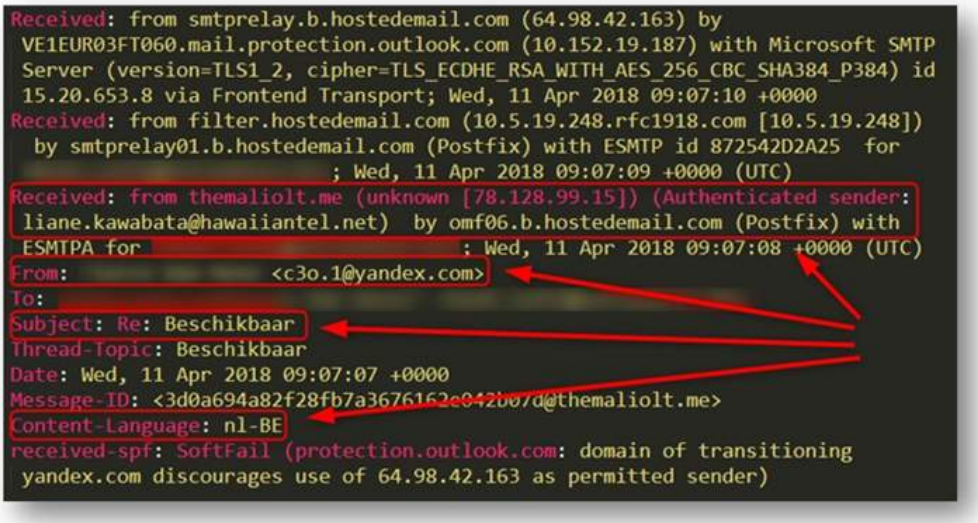
Gelieve 23,800.00 euro naar onderstaande bankrekening gegevens over te brengen;

bedrag: EUR 23,800.00
Naam van de bank: DBS BANK LTD
Naam van de rekeninghouder: ZH-NET ENTERPRISE LTD.
Swift code: DHBKHKHH
IBAN/Acc: 016-478-783143372
Bank adres: 11/F, The Center, ????? 99 Queen Road Central, Hong Kong

Met vriendelijke groet,

4. ANALYZING THE HEADER

In the following screenshot, the indicators are marked in RED.



We can see the email has been sent from an IP originating (**78.128.99.15**) most probably from Bulgaria.

Even if the “FROM” (and “REPLY-TO”) indicates an address **@yandex.com**, the mail has been sent with an authenticated sender **@hawaiiantel.net**.

These points will be investigated further below.

5. INVESTIGATION

We have several points to verify:

- **Distribution list**
- **Source IP:** 78.128.99.15 (themaliolt.me)
- **Authenticated sender:** liane.kawabata @hawaiiantel.net
- **FROM/REPLY address:** c3o.1 @yandex.com
- **Banking information’s:** Bank and account holder

Distribution list

We can make some correlation from the different cases which were reported.

Each case was about companies from the same sector. Those companies are using the same website layout, where the name, role and email address of the CEO and his collaborator are easy to find.

In the company profiling, the collaborators can be either secretaries or accountants.

The list of these websites can be found in a central directory, also publicly available.

Knowing this, it was only a matter of time for a hacker to script an automated extractor, to build his distribution list.

Source IP

The IP source comes from a Bulgarian subnet of 255 IP addresses, containing, among other things, a Tor relay (78.128.99.22).

```
% Information related to '78.128.99.0/24AS203380'

route:          78.128.99.0/24
origin:         AS203380
mnt-by:         dagroup
mnt-by:         AZ39139-MNT
created:        2017-11-22T16:08:39Z
last-modified:  2017-11-22T16:08:39Z
source:         RIPE
```

Searching more specifically for phishing indicators, we can see several hostnames linked to phishing campaigns on our phishing IP.

IP 78.128.99.15
Country Bulgaria
Network Telehouse EAD
AS 8877

- 66E693506CE51B6562F93E62C780DBF1
- 1AFB49ED954B08D8F1BDAFFB906283AB
- 1E2AADA837946F1FBA90D1DDD08F566D
- 449D35A22FFC4B260704B32868C103A2
- 4CA9C28BA407915FA62EE7651F9BE441
- 974B13000C4EDF846C28D41DC4165EA1
- 5CFF518F08AEA8BBCCEEF7F684CF7930

	URL	MD5	IP		Threat
2018-04-12 23:56:22	http://mykallott.org/way/owo/38f467b8480969bd47...	58F2F661A037C7DF75FB8341688D7B7E	78.128.99.15	BG	JS/Phish
2018-04-12 21:17:16	http://skintfm.net/cgi-ssl/admin-vendor/efax-pd...	86E99CE1A8ADAA2DAA8FACED5F29311B	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-11 23:08:13	http://mykallott.org/way/owo/38f467b8480969bd47...	58F2F661A037C7DF75FB8341688D7B7E	78.128.99.15	BG	JS/Phish
2018-04-11 14:58:24	http://skintfm.net/cgi-ssl/admin-vendor/efax-pd...	AE490BA98AA8A604CD82253CC2F6F868	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-11 13:10:24	http://thekallott.com/wels-log/auth-log/Home/Fi...	89B6ACF89343B78554ED34E0A2CCE4B3	78.128.99.15	BG	XPL/Gen.BW.1701_31
2018-04-10 10:56:25	http://skintfm.net/cgi-ssl/admin-vendor/efax-pd...	AE490BA98AA8A604CD82253CC2F6F868	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-10 10:31:41	http://skintfm.net/cgi-ssl/admin-vendor/efax-pd...	AE490BA98AA8A604CD82253CC2F6F868	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-10 09:53:45	http://skintfm.net/Dior/login.microsoftonline.c...	782598E673FDA65A4BA425F98E2C97E0	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-10 08:20:08	http://skintfm.net/Dior/login.microsoftonline.c...	AE490BA98AA8A604CD82253CC2F6F868	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan
2018-04-10 08:14:39	http://skintfm.net/Dior/login.microsoftonline.c...	7C0031DE5940D55762DAC4F5D7796FBB	78.128.99.15	BG	HTML/Phishing.Agent.EW trojan

What we can conclude so far, the hacker has most probably used some kind of bot from that IP to send the initial phishing emails.

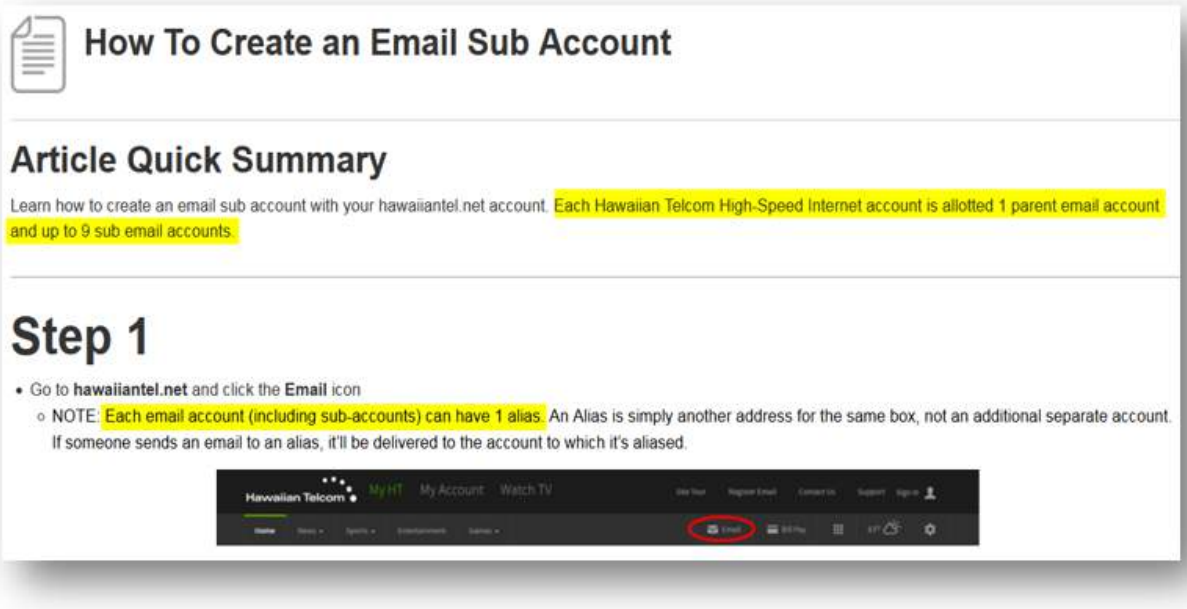
Authenticated Sender

The mail has been sent using a regular mail from an Internet Service Provider located in Hawaii (Hawaiiantel).

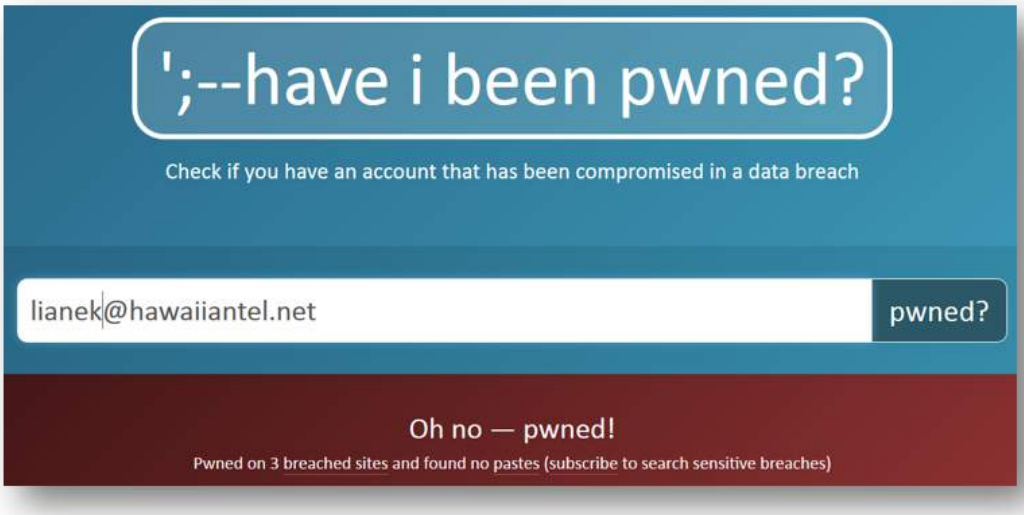
Looking on public leaks, hundreds of emails account from that ISP has been leaked.

But this one doesn't seem to have ever been leaked. However, is it sufficient to identify who the hacker is?

The FAQ of the ISP can give us some other hint. Potentially, from 1 account, a user can have up to 20 email addresses.



After some social engineering, we can determine the main account address. Another check will confirm our assumption that the account should have been hacked.



The email used to send the first mail is either an alias or a secondary address of **lianek**.

Using a real ISP email address, the hacker is lowering the risk of the incoming mail to be blacklisted. We will now see why the hacker has used another account for the replies.

FROM/REPLY address

The problem while using a stolen email account is the possibility to lose the stolen account once it's discovered.

A lot of replies on a stolen mailbox can be suspicious to the legitimate user. The hacker must be as quiet as possible, reason why the answers are to be received from another mailbox (here, on "yandex.com").

Depending of the size of the phishing campaign, the requirements are:

- Size: No limitation on the mailbox
- Registration: avoid using any "private data" to create an account (other email, phone number, …)
- Intrackability: ability to use Tor to use the email, and location outside EU
- No cost
- Usable without webmail (automation …)

The table below will give some pointers on Yandex (src: https://en.wikipedia.org/wiki/Comparison_of_webmail_providers).

Product	Yandex Mail
Owner	Yandex LLC
Cost	Free (Ad)
Mailbox storage	Unlimited
Supported languages	10
POP3[lower-alpha 1] **support**	Yes
IMAP support	Yes
SMTP support	Yes
Cryptographic protocol support	SSL, TLS
Account expiration (inactivity)	24 months
Can create email without cellular or email verification	Yes
Server's location(s)	Russia
Secure (SSL) webmail	Yes (default)
Tor browser allowed	Yes

The last point, while creating an email address on Yandex, we can choose for either a @yandex.ru or a @yandex.com.

Obviously, using a ".com" looks even less suspicious …

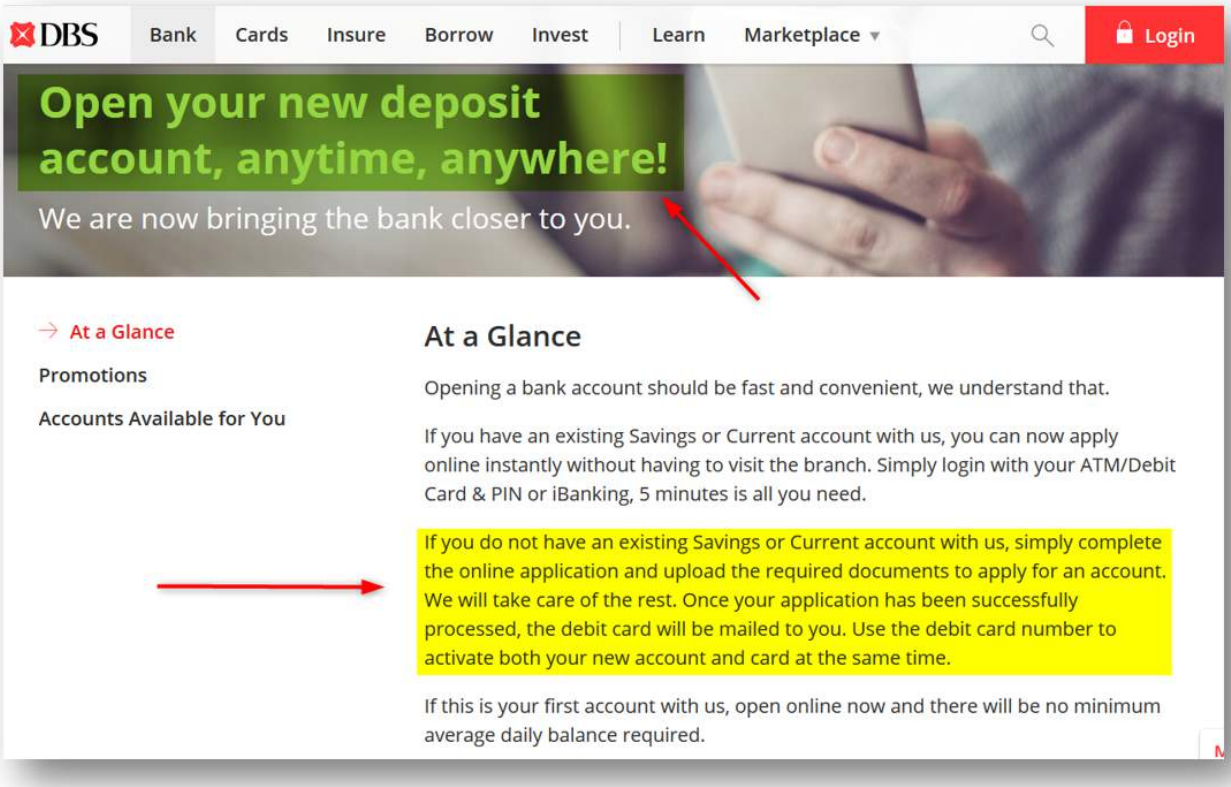
Banking information's

We have 2 points to verify here:

- Bank: DBS BANK LTD.
- Account holder: ZH-NET ENTERPRISE LTD.

The choice of the bank is quite explicable as the online creation of a bank account at DBS can be done very simply.

The only information asked is a passport number, but **without in-depth verification**. Any passport number found on Internet (e.g. Pastebin) is sufficient to create an account.



The last information coming from the phishing mail concerns the holder of the bank account. As there is no verification of the account, any name can be used. Here, the name which was used is one of a Trading Company, specialized in import/export, which would seem legitimate.

6. CONCLUSION

In this article, I've tried to show how a targeted phishing attack can be thoroughly prepared and executed, and how hard it can be to respond accordingly and identify the hacker.

As a bonus, down below, you will find some general advices to help you while receiving phishing emails.

7. HOW TO RESPOND TO PHISHING

Always be careful when using email

- Verify thoroughly the source (FROM) AND responder (REPLY-TO), not only the name printed (View header message on Outlook, Thunderbird, Mail).
- Don’t open an attachment blindly nor click on a link if the source is not verified.
- Beware of emails requesting personal information (usernames, password, …)

Track spelling errors and typos

- Can be an indicator of mass phishing email

Be extra cautious on urgent action

- Watch out for calls to action with deadline as attackers use time sensitive and threatening language to increase the chance of action
- Whenever you are in doubt, check the information using another medium (phone, face-to-face, …)

8. About Approach

Approach is a specialised cyber-security company providing services to business and public customers.

Our customer base ranges from start-ups and SMB's to the world's largest corporations and public institutions.

Our uniquely broad spectrum of expertise enables us to propose a global approach to cyber-security.

We offer services and solutions covering the entire cyber-security value chain, from governance and strategy through to resilient technical designs, architectures and implementations.

Because we have our own software factory, we are uniquely positioned to develop highly secure solutions for our clients.

We are continuously investing in our talents and developing the skills of our people. We use the best technologies available so that we can be even more effective.

Our company headquarters are located in the NewTech area of the Axis-Parc close to Louvain-la-Neuve

You can find us on , , or on our website: www.approach.be

9. About the authors

Dimitri Diakodimitris
Cyber Security Senior Consultant at Approach Belgium