TRIMOS

PHISHING SAFETY TIPS

Swiss Measuring Instruments

Table of contents

1 Context

We currently observe an increase in phishing attempts targeting our agents. Most of the times, these mails try to spoof Mr. P. Kemper e-mail address or another member of the general management. The goal behind these mails is to, sooner or later, lure our agents into making a payment on an unusual bank account controlled by the attackers.

Once the payment is done, there is close to zero chance to recover the funds, as they will be immediately redirected elsewhere until the track is lost. Therefore, it is really important to avoid paying any amount when there is the smaller doubt regarding the genuineness of the request.

2 How to spot a phishing mail

Phishing attempts vary widely in sophistication. Most of the times they are easy to spot, but sometimes not. We can split the analysis of a mail into two parts: the headers and the body.

While less common, it can happen that a legitimate mail account has been compromised. In this case the mail is authentic and the only way to tell something is going wrong is common sense.

2.1 Mail body

The contents of a phishing mail can vary greatly but most of the times we find some of these recurring patterns:

- Sense of urgency (ASAP, urgently, …)
- Unusual writing (unusual tone, grammar / spelling mistakes, unusual signatures)
- Unusual requests (change in payment method, unusual bank account, …)

As mentioned above, the ultimate goal is to trigger a payment to an unusual bank account, almost never on our swiss bank accounts but in overseas banks like HSBC.

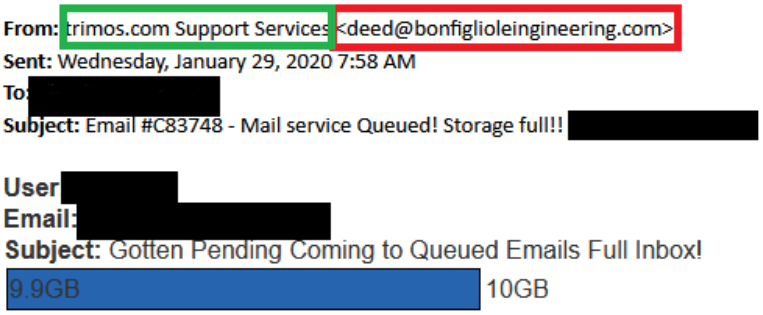
2.2 Mail headers

A classic scenario for phishing is a technique called e-mail forgery. The classic (and old) SMTP mail protocol allows the sender of an e-mail to specify himself all the headers, including *MAIL FROM*, which allows to show any e-mail address as the original sender.

Fortunately, there are ways to tell if the mail really comes from the labelled sender. However, depending on the phishing sophistication, reading the source code of the mail may be required. The best approach when unsure is to carefully read the mail and look for obvious spam evidence. Then, if nothing seems wrong, the ultimate check is to read the mail source but it may not be easy for everybody. We will see some example here to help with this process.

2.2.1 Obvious spam evidence

Sometimes, the fake sender e-mail address can be seen directly in the mail. The full sender name seems legit (here in green) but the e-mail address doesn't match it and most of the times looks not very professional.



That's why it is really important to look carefully first for a suspicious address. Unfortunately, some mail forgeries are more sophisticated and need source examination.

2.2.2 Spam evidence in mail source

Recently, we've been informed that some of our agents were receiving fake mails similar to the one below.

The sender address in green looks legit (except the unusual upper-case letters but it is arguably still legit). However, the mail body is highly suspicious (notice for instance the *asap*). In this case the signature is not Mr Kemper's usual one but anyway it could very well be the case.

This is a perfect example of mail forgery. The only way to tell for sure it is a phishing attempt is to look at the source. Below is an extract the source of a similar e-mail received by one of our agents.

```
    by ofmgw0252.ocn.ad.jp (Postfix) with ESMTP id 7074B1300244
    for [redacted]; Mon, 27 Jan 2020 19:23:58 +0900 (JST)
Received: from trimos.ch ([13.82.128.125]) by :SMTPAUTH: with ESMTPSA
    id [redacted]; Mon, 27 Jan 2020 03:23:56 -0700
X-Sender: sender@5ymail.com
Date: Mon, 27 Jan 2020 10:23:55 +0000
To: [redacted]
From: Patrice Kemper <P.Kemper@trimos.ch>
Message-ID: <ef05d1746282232f97b166aab9133a58@trimos.ch>
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="b1_ef05d1746282232f97b166aab9133a58"
Content-Transfer-Encoding: 8bit
X-CMAE-Envelope:
MS4wfABfHzO45itIbwP7yrUJihFTze7Jaa4GXEqGIHWVmSAFELyt2GvullW2Gkb9/Mi48qy8
    tMHhMJOFSGTpuGg1dsRYbqerblfQ8B91O7QUBn7jU7fiRrok+jqdI6Kf
Subject: [ ML ] Trimos SA Rep/Distributor
X-BeenThere: [redacted]
X-Mailman-Version: 2.1.12
Precedence: list
Reply-To: Patrice Kemper <cruisejoy2846291@outlook.com>

This is a multi-part message in MIME format.

--b1_ef05d1746282232f97b166aab9133a58
Content-Type: text/plain; charset=us-ascii

Hello,
How are you doing today?Do you have a moment to chat on email?I hav
asap.
Regards,
Patrice KemperMD/Chief Executive Officer (CEO)
Trimos SAAv. de Longemalle 51020 RenensSwitzerland.
```

The parts in red show that the message is a phishing. First of all, the sender identifies itself as being *trimos.ch* (*MAIL FROM* field in *SMTP*) but has actually nothing to do with Trimos. In fact, *13.82.128.125* is an American IP Address owned by the anonymous mail platform *5ymail.me*.

IP Information for 13.82.128.125

– Quick Stats

IP Location	United States Of America Washington Microsoft Corporation
ASN	AS8075 MICROSOFT-CORP-MSN-AS-BLOCK, US (registered Mar 31, 1997)
Resolve Host	5ymail.me

Then, we clearly see the real sender is *sender@5ymail.com*. Finally, we see the real return address *cruisejoy2846291@outlook.com*. In fact, when replying to this mail, this strange address will appear and should alarm the target of a phishing attempt.

As we can see, the source of the mail provides enough evidence of phishing. However, reading the source of the mail is not something everybody can do with ease. That's why we recommend to follow the advices provided in chapter 3 *How to help prevent Trimos-based phishing attempts*.

2.3 Compromised mail account

If a legitimate Trimos mail account has been compromised, reading the source will show no evidence of phishing. In this extreme case, the only way of spotting a malicious e-mail is to analyze the mail body and rely on common sense and indications on Chapter 2.1 *Mail body* to make a decision.

2.4 What to do if in doubt

When in doubt the best option is to contact Trimos directly, preferably by phone.

In any case, never make payments to non-standard bank accounts. **We do never change our bank accounts**.

3 How to help prevent Trimos-based phishing attempts

In order to authenticate outgoing mails form our servers, Trimos implements both **SPF** (*Sender Policy Framework*) and **DKIM** (*Domain Keys Identified Mail*) authentication methods.

If the receiving mail server enable checks for these both methods, risks of receiving a Trimos phishing mail are greatly reduced. Thus, we recommend you to check with your IT department or mail providers if it possible to implements both of those methods.