****

**INTRODUCTION**

**E**mail is supposed to enhance business communication. But the reverse becomes the case when communication between a *seller* and a prospective *buyer* is interrupted by somewhat sophisticated *fraudsters* in a manner that can be described as a “*man in the middle attack”.* Internet communications are not always secure. There are lots of attacks here and there on Information systems around the world, and with Email being a significant target… online B2b participants are better off armed with information that will help them protect their business information from prying eyes.

This presentation seeks to unravel the modus operandi of Business to Business(B2B) scams that currently plague international businessmen in established online B2B platforms.

**WHY WE NEED EMAIL?**

Email will remain hugely significant, surpassing Telephony and Postal Service as a communication tool in the B2B ecosystem- due in part to speed of delivery and ability to deliver messages together with necessary business documents (*as attachments*) in several ubiquitous formats, but also because phone calls between people of different languages and cultures (*as is usually the case between buyers and sellers in B2B scenarios*) do not give enough room for expression of interest and offering as a result. With email there is enough time for a seller to scrutinize a buyer’s request for quote and as such present a suitable offering. Email will remain the Ideal business communication tool

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**AN INHERENT PROBLEM**

This inherent strength of Electronic mail is also matched with as much weakness. Email is overly insecure as we will see in this report. There is no unobtrusive way for a person who receives a message to ascertain that the message came from where it claims to have come from. For an international businessman who leverages the Online B2b marketplace and Electronic mail, A proper and useful combination of the three business communication tools highlighted above is what he/she will need to ensure that communication between his buyers and/or sellers are effective but also secure. One will not be able to rely on email alone except you adopt certain preventive strategies as will be shown in the accompanying presentation.

Salesmen and other business communication personnel who do not acknowledge the presence of email scams in online B2B marketplaces will remain a sitting target for costly security attacks resulting in huge financial losses.

**EMAIL SCAMS IN B2B MARKETPLACES- THE EXPOSE**

**O**nline B2B marketplaces usually require Sellers (*Suppliers, Companies,and Manufacturers)* and Buyers to register and create their profiles online. As part of the registration, the Buyer or Seller is required to provide an email address that will serve as messaging tool in the course of their transaction with other buyers and sellers. Registrations are usually free so there is little or no investment required by intending fraudster.

The Scam Modus Operandi goes thus;

1. Sourcing: Like every normal buyer a Scam Buyer will source for products from suppliers using search provided by an online B2B marketplace. After search results show up, the scammer checks the companies that appear with every search result and asks for a RFQ. The aim here is to contact as many suppliers as possible in a process nicknamed **BOMBING** ---show images from alibaba.com…europages.com…globalsources.com…

Thus increasing the chances for successful attacks.

1. Messages of RFQs together with contact information of the buyer are automatically sent to all the sellers’ email addresses - obviously the email addresses they provided in the course of registration as members of the B2B marketplace. The idea is that the sellers will thereon have to contact the buyers directly. One thing to note here is that RFQs from Scam Buyers are never detailed and the seller is moved to write the buyer to ask for more details like a picture or any document describing the product in the request. This is where it all heats up.
2. **Phishing**: In this stage the scam buyer tries to steal the password of sellers using the effective phishing techniques or other more sophisticated Trojan-Horse botnet attack.  
   below is an email message from a scam buyer to a seller in reply to the seller’s request for more details discussed in 2. above

…

2nd format…in a mail program showing link and attachment

…

In a phishing attack the seller is required to click a link or download an attachment in the message to view the detailed specifications of the buyer’s request. The link directs the seller instead to enter his password into a login screen that has a striking resemblance to the original login screen that they use in gaining access to their inbox

*(Visit* [*http://www.kennethetal.com/b2b-scam-expose/phishing-pages*](http://www.kennethetal.com/b2b-scam-expose/phishing-pages) *to give yourself a feel of the phishing attack)* … discuss spyware if necessary or state that its outside the scope of this work.

For an unsuspecting seller the result is loss of password to fraudsters as they are redirected to some page on the worldwide web where they left to wonder what to do next until they give up on the buyer and move on.

1. Armed with the passwords to email address of sellers (*usually the sales department email*)the scammer gains entry into the inbox of the seller and this is where it all heats up. After studying messages in the Inbox and Sent Folders of the seller,the scammer makes a list of all buyers who have indicated a genuine interest to buy and pay for goods being produced for them. A mind blowing trick nicknamed **CLONING** follows.
2. **Cloning** involves exploitation of common sense. To clone an email address the scammer creates an email that has a striking resemblance to the sellers’ email for example

Looking at an email address [wangcho@gmail.com](mailto:wangcho@gmail.com) a clone [vvangcho@gmail.com](mailto:vvangcho@gmail.com) will be created.

Looking closely, you will see that the first email address begins with a “w” whereas the second email begins with a “v” followed by another v that makes it look like a “w”