

1st January, 2014

Preventing Today's Email Fraud

by Marcus Low, R&D Director

Email fraud, its more rampant than one would think. Over the last few months, InternetNow have looked into a number of cases related to email fraud. In one of the cases, a company headquartered in Shah Alam lost out on over USD6,000 payment. While in the another case in Ipoh, USD7,000 payment was lost and a Klang setup have to write off USD 70,000. Due to the sensitivity of these incidents, all names are held confidential.

The modus operandi in all these cases are identical. The fraudsters snooped to the email conversations between the company and their clients. And then when any payments are about to be made via bank transfers, they would send a carefully crafted email to deceive the client into paying into a different bank account.

How is this even possible?

First of all, email by design is not secure. It was meant to be a form of text transportation where functionality of

such mechanism and interoperability was given priority and security taking a backseat. Earliest email encoding proposal existed since 1970s and evolved into primitive internet usage in the 80s.

Mails that we send today are not encrypted, meaning they can easily be read before they reach the recipients. So that means even your IT department or email provider can easily reach your emails.

Many email systems today are also accessible from outside the office network. This makes it easier for fraudster to gain access to various email accounts, especially if the accounts' passwords are weak and subjected to simple attempts. Exploits on existing platforms and common softwares used for emails and hosting are targets to gain access to the system and ultimately passwords of users in mail systems.

Example of Vulnerabilities of Apache/IIS used by almost all hosting companies (note the date): (refer image 1 &2)

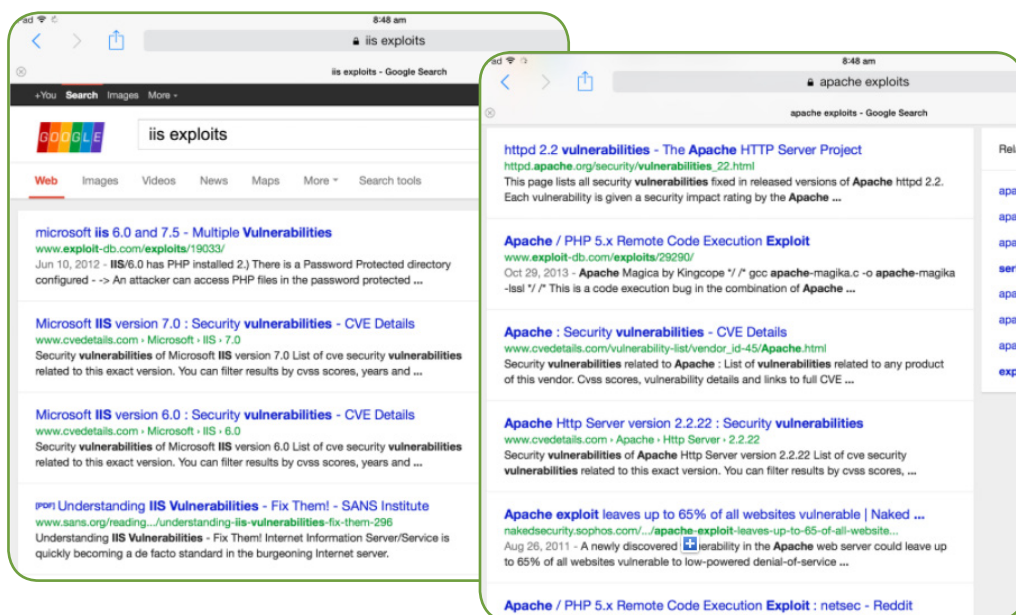


Image 1 & 2: Example of Vulnerabilities of Apache/IIS

Finally, malwares are getting more sophisticated today. Once planted on a user computer, many are capable of forwarding emails stored in popular email programs to the fraudsters or at least allows them to have access to the content.

Majority of transactional emails whereby information regarding banking in of funds and invoices are handled by staffs that are in the financial fields such as accounting or financial administration

and often lacks the technical mentality required to identify the fraud email.

A combination of any of these factors along with social engineering creates many opportunities for the fraudsters to begin their operations.

Solution : Secure the communication

If one party have to pass something of great value to another party, assuming the object of value is a brick of gold, how would one proceed to do this. One would not just publicly pass the object around, nor leave any hint to the existence of such an object. In fact, the party holding the object would ensure only the person that he/she knew would be the one receiving the object and not any other parties. The party holding the gold would setup a secure site to meet and deliver the gold.

In digital world, the components at play would be : Encryption and Secure medium. Although these normally would require complex setups, the solution proposed here would not only be effective but easy to establish.

To communicate securely, email encryption has to be utilised. It ensures that the email sent is not read visibly by the public or anyone having access to the compromised machine.

Implementation Challenges

While email encryption technology such as S/MIME, PGP have been around for decades, they are not very popular amongst laymen users because of user-unfriendliness

Apart from being complicated to install and operate, they require both parties to implement such technologies

So even if a company decides to use encryption but their clients has no such system, secured email communication is not possible.

The Solution Now



Antispameurope offers user-friendly email encryption that is automatically triggered by specific recipient at the sender's will. Financial staffs involved in transactional processing can send normal emails and encrypted emails depending on who the recipient and specific email. For e.g: all invoices could be sent encrypted to XYZ.


Antispameurope offers an email encryption technology called WebSafe. **It does not need the recipient side to install any encryption system** to function.

When a user sends an email using this technology, the email will be encrypted and stored securely on antispameurope server. European data centers adopts have strict privacy policies and does falls into any "patriot act" or influence of NSA.

The recipient will not receive the encrypted mail. Instead a mail such as the left (refer image 3) will be delivered. It contains a link to the secure site where the email is stored.

◀ *Image 3: The recipient will receive a mail which contains a link to the secure site where the email is stored.*

Invoice #8 WEBSAFE (Websafe Encrypted)
7 February, 2014 9:51 am



Willkommen beim antispameurope Verschlüsselungsservice

You have received a confidential message.

Datum: "07.02.14 02:02:09"
Von: "marcus@internetnow.com.my"
An: "marcus.is.good@icloud.com"
Betreff: "Invoice #8 WEBSAFE"

In order to safely deliver the message to you, a user account has been created for the antispameurope websafe
With the following link you can access the email:

<https://control.cloud-security.net/websafe/ws.php?code=ebd75ec7ac5b95661a22b4d7714759d4>

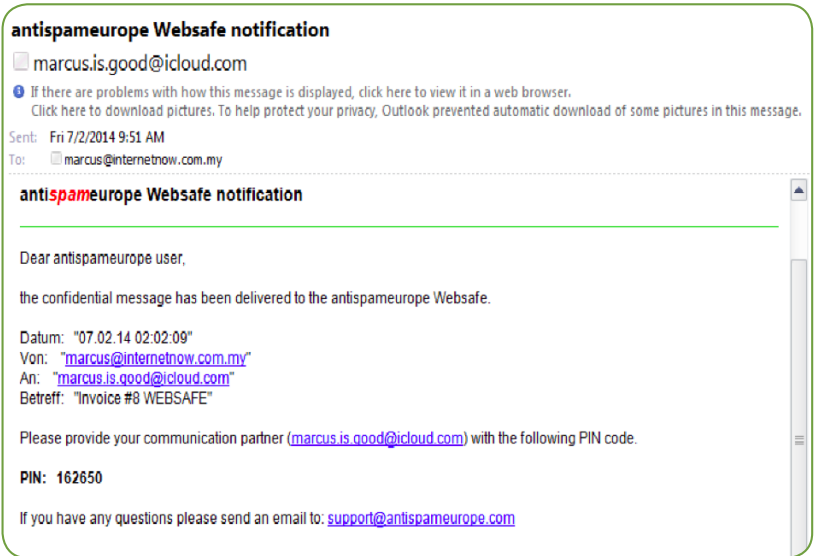
If you are using the Websafe for the first time, **you will need the PIN code** provided by your communication partner (marcus@internetnow.com.my).
If you have any questions please send an email to: support@antispameurope.com

Sincerely,

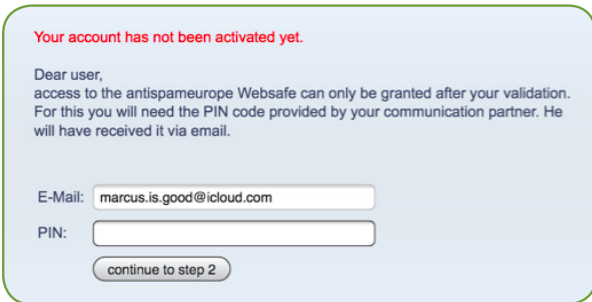
Your antispameurope team
Tel.: +49 511-260 905-50
E-Mail: support@antispameurope.com
Web: www.antispameurope.com



Upon clicking the link the user will be directed to a site like below (refer image 5) where a PIN needs to be entered. The PIN would have been sent by the sender (refer image 4) earlier via a separate channel such as SMS, fax or over the phone. This is to establish that the other party is exactly who the user is authorizing to be part of this secure communication and needs to be done only once. Since the PIN is only accepted once, fraudster could not use the PIN even if he/she have access to it somehow because then the actual party would not be able to use it and raises suspicion immediately.



▲ Image 4: The sender will received a PIN by the sender (image 4) earlier via a separate channel such as SMS or over the phone

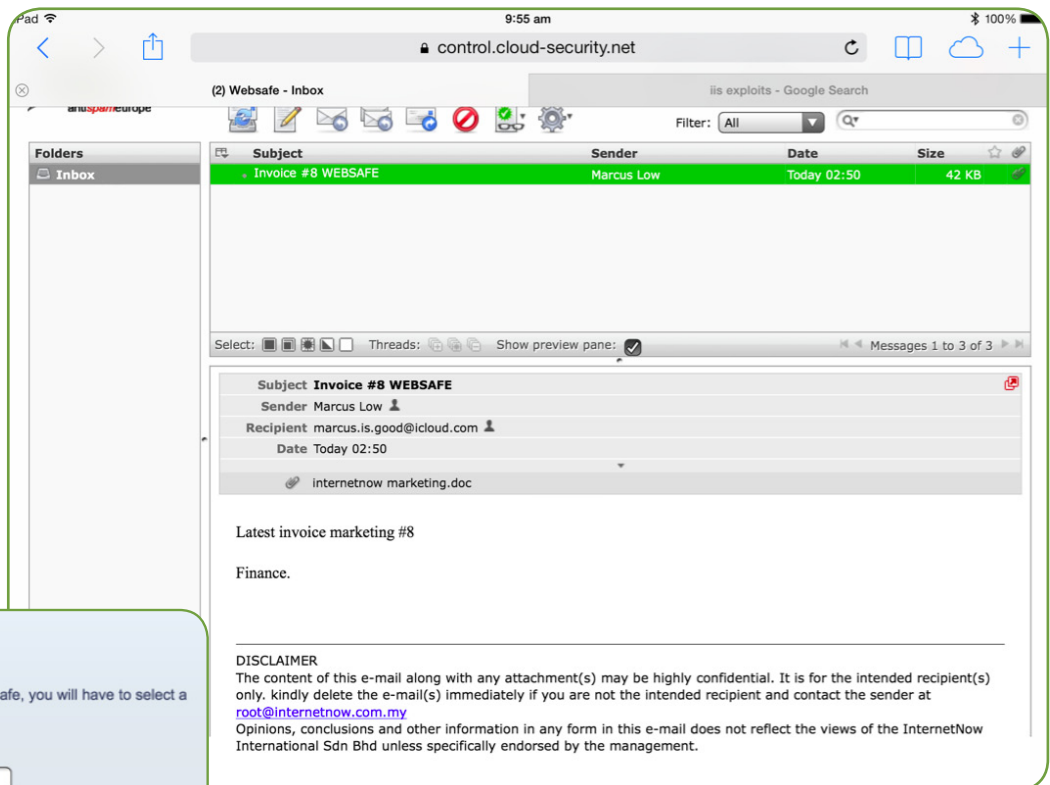


◀ Image 5: User will be directed to a site where a PIN needs to be entered.



Once the correct PIN is entered, the user will be able to enter the WebSafe

webmail (refer image 7) where all the encrypted mails can be read. Other email activities, such as replying, can also be done securely on this site. At this point the verified user is asked to create his/her own password to this secure medium. (refer image 6)



▲ Image 7: Websafe webmail where all the encrypted mails can be read.



▲ Image 6: verified user is asked to create his/her own password

Conclusion

The rising cases of email related fraud requires serious attention by IT departments and company owners. The financial and reputation damages easily outweigh the cost of investing in secure encrypted email.

Existing email encryption solutions are cumbersome and not user-friendly. Furthermore they do not work if the recipient side does not have such system.

Antispameurope WebSafe email encryption has various key benefits:

- ✓ It still works even if the recipient side does not have email encryption
- ✓ It does not depend on expensive email certificates
- ✓ It is able to support legacy encryption technology such as TLS, S/MIME, PGP if required.

NOTE: Marcus Low can be contacted via +6 012-3766 367 OR marcus@internetnow.com.my

*InternetNow is the distributor of antispameurope for South East Asia. Resellers are welcome.
Contact us today at enquiry@internetnow.com.my*