Theron Le Roux
Accountants I Rekenmeesters
We care about your business
Assosiaat Algemene Rekenmeester (SA • Associate General Accountant (SA)
Professionele Rekenmeester (SA) • Professional Accountant (SA)
Belastingpraktisyn • Tax practitioner
38 Akasia Street George East 6529 • ✉ 4529 George East 6539 • Tel: 044 871 5067 • Fax: 044 871 5082 • Email: jgmt@jgmt.co.za

# ACCOUNT HIJACKING WITH USE OF SPYWARE

We are encountering an increasing number of cases where clients fall victim to sophisticated types of spyware used for Account Hijacking (ACH). The more "traditional" scams consisted of the following broad types (described in broad terms and in layman terms):

1. The perpetrator would send you an e-mail from your "bank", containing a link to "update your detail or perform some training". This link took you to a falsified or spoofed website. As you enter your account number, Pin and Password your security detail is harvested. If you fall victim to this type of scam, the financial institutions or your insurance consider it to be negligence and might not refund your money. Knowledge and alertness is the only sure way of eluding this threat.

2. Spyware is installed on your computer by a person having access to your computer/network or an executable file is e-mailed to you. The spyware, once installed, captures all your keystrokes and this information is used to access your finances. If you fall victim to this type of scam, the financial institutions or your insurance consider it to be negligence and might not refund your money. A good anti- virus/spyware program, knowledge and alertness will greatly assist in ensuring that you elude this threat.

3. The newer type of attack, which is frightfully successful, consists of the following: An e-mail message is sent to you with a zip file attached, named "Proof of payment". (a virus/spyware in a zip file has a better chance of not being blocked by the firewall). If you open the zip file it contains a pdf file named "Proof of payment". Normally a pdf file is considered to be harmless and can be trusted. If you open the pdf file it is empty or gives an error message! This pdf is in fact a spyware executable file, disguised with a pdf logo! When you open the file it actually installs the spyware program on your computer which captures all your keystrokes. The program is very advanced (sophisticated) in that it can be programmed to create a backdoor on your computer, re-install itself with new file names and uninstall itself after a period. This makes it exceptionally difficult for virus protection programs to detect it. We scanned it with 4 of the major commercial virus/spyware protection programs and none of them detected it. In a number of cases that we have investigated, the clients' money was not refunded, although, we are of the opinion that nothing more could have been done to protect or prevent this breach. We are awaiting the final verdict in these cases. We are of the opinion that this threat is one of the most serious threats to businesses due to the sophistication of the spyware being used. There is very little defense against this type of attack. Through the assistance of one of our Cyber Crime experts we are able to provide you with a list of recommendations on how to better protect your organisation against spyware and Trojan attacks in general.

**RECOMMENDATIONS TO CLIENTS TO PREVENT THE LOSS OF FUNDS DUE TO SPYWARE AND TROJANS**
**RESULTING IN FRAUDULENT EFT'S**

These are generic steps and would not all apply to your specific environment.

**SECURITY MEASURES ITO PERSONNEL**

1. User names and passwords must be in-line with acceptable guidelines i.t.o. usernames and passwords.

2. Passwords on financial systems should be changed on a weekly basis and not on a monthly period like normal users.

3. Financial users must attend a security awareness training session to be made aware of the methodologies and modus operandi which the syndicates follow and to identify suspicious activities/actions on their computers.

4. A specific user may only load transactions and specific users may authorise them.

5. Security checks should be done on financial personnel.

6. Security personnel should be submitted to polygraph tests on a quarterly a basis.

**SECURITY MEASURES ITO FINANCIAL PERSONNEL'S COMPUTERS**

7. The financial computers should have a very good virus/spyware protection programs installed. More than one program must be installed on the IT systems to detect malicious software. Anti- Virus and two other programs (Anti-malware) must be installed on all computers used to conduct Internet Banking.

8. The databases of these virus/spyware protection programs should be updated daily. The updates must be done from a centralized server and then updated to the computer each time it logs on to the network. This will prevent suspects from excluding the spyware from the local anti-spyware database and still provide security even if the user forgets or prevents the backups.

9. Alerts arising from the above programs must be investigated to verify that malicious applications were stopped and that the threat was investigated.

10. Flash Drives (Memory Sticks) must not be allowed to be used on these allocated computers.

11. Only one security cleared IT support person may work on the computers of financial personnel.

12. No e-mails should be sent or received on computers used for Internet banking.

13. Financial computers must be kept in a secure environment with access control to the area.

**SECURITY MEASURES ITO THE FINANCIAL SYSTEM**

14. The processes and banking system must be setup in such a fashion that the loading and authorization of transactions must be at least 24 hours apart. This will give the person's the opportunity to verify transactions and discover fraud. We see that he syndicates load and authorise transactions normally within 30 minutes of each other.

15. The banking system must only affect the transfer of the money after a period of three days after it was approved.

16. No monies may be paid over to a beneficiary within three days after the banking details were changed.

17. No monies may be paid to a beneficiary who was created within 5 days prior to the payment.

18. Transfers may only be loaded and authorised in office hours.

19. Password changing must only be allowed in office hours before 15h00.

20. Internet Banking must be limited to 2 or 3 computers. These computers must be setup with fixed IP Addresses and Computer Names. The security to access these computers must be regulated by at least 2 security devices eg password & token or biometric device.

21. The user profiles of Users who have resigned must be deleted not just suspended.

**SECURITY MEASURES ITO THE BANK**

22. The Bank must alert the employees (Specific employee who login to the Bank) and the office head (Financial Manager or Chief Financial Officer) by SMS (Short Message Service) and\or electronic mail (e-mail) regarding Login to the Internet Banking Service.

23. The Bank must alert at least two persons (person making changes and the person authorising the changes) by SMS (Short Message Service) and\or electronic mail (email) regarding changes (new

information added or altered) on the Bank's Internet Banking Service. The Bank Internet Banking Service does not initiate any password changing for employees.

24. The Bank must initiate password changing once every 7-14 Days. Alert of the password changing must be sent to at least two persons (person changing his/her password and the office head) by SMS (Short Message Service) and\or electronic mail (e-mail) regarding the password changed.

25. The Bank must configure their systems to allow only the computers containing the above details with regards to the IP Address and Computer Names.

**ACTIONS TO TAKE WHEN A FRAUDULENT EFT IS DISCOVERED AND SPYWARE IS SUSPECTED.**

26. Call a computer forensic expert immediately. Do not take any actions, as below, before obtaining the advice of the expert.

27. The computers which are suspected to be invested must not be used further do not switch it off, leave it as is.

28. Change all financial personnel's passwords from another computer.

29. Institute interim manual procedures to verify the loading and authorization of all financial transactions.

30. Limit the number of people and computers who can access the banking.

31. After forensic copies were made of the invested computers, spyware scans must be run and the spyware removed. Establish the reason why the anti-spyware programs did not identify the spyware.
32. Notify the bank of the fraud and request vigilant action from their side.

33. All information of the fraudulent transactions and all history of the compromised user accounts must be requested from the bank immediately.

34. The funds must be traced and frozen and a letter of demand must be sent to the bank(s) to recover the funds.

35. A Criminal case must be opened a.s.a.p.

*Compliments from Danny Myburgh – Cyanre ACFE SA Cyber Forum Chair*