Dynamics and methods of a forensic analysis on an internet banking fraud case

"Wilson Leite da Silva Filho (a), Romulo Soares da Silva (b),"

***Abstract*—This article presents the dynamics and methods used in a real forensic investigation case related to Internet Banking Fraud.**

Based on the information reported to the police force and the suspect's computers apprehended at the suspect's house, the criminal experts performed a series of forensics analysis in order to find evidences that could link the computers to the investigated crimes.

***Keywords*—Internet banking fraud, phishing attacks, cyber crime investigation;**

1. Introduction

Banks are one of the main targets of the cyber criminals that want to make some easy money. Nowadays, banking activities and transactions are fully available through the Internet. The amount of money that is available by the net calls the attention of these criminals.

Although banks invest hard in security, the criminals are always trying to figure out a way to overcome the security mechanisms adopted by the financial institutions.

The easiest way found by these criminals to break the security is to target the final user. This kind of attack uses the information technology with some social engineering to fool the users into doing some procedures that compromises the security of the banking transaction done in their personal computers.

The previously mentioned kind of attack that uses both technology and some social engineering is known as phishing. In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication [4].

Howard et al [1], classify the malwares used to compromise sensitive user data according to their capabilities and degree of sophistication. They classify the types of malware as keystroke logging, form grabbing, screen-shots and mouse event capturing, phishing and pharming Trojans, HTML injection, protected storage and saved password retrieval and certificate stealing.

In this article, the authors present the dynamics and methods used in a real forensic investigation case related to Internet Banking Fraud against one of the top five Brazilian banks.

2. About the banking fraud case

The case study presented in this article is based in a real case analyzed in the crime laboratory of the Criminal Institute.

The bank received several complains saying that money was being improperly transferred from their customers' accounts. Once the bank security technology team confirmed the complaints, they called the police. The police traced the IP addresses informed by the bank to an Internet Service Provider (ISP). The ISP informed the residence address of the IP owner. Then, the police went to this address and apprehended the computer material that was there.

The criminal experts received at the lab four computers supposedly involved in the banking fraud. The preliminary information received by the experts informed that amounts of money were moved from bank client accounts and used to pay federal taxes of a third company that may be involved in the crime.

The police authority formulated several questions about the activities performed by the computer user. Among them the police authority asked if there was some evidence of malware software; if there was evidence of fraudulent bank access; if there was evidence regarding federal taxes documents that would be paid with the victims' money.

Based in the description of the case and the questions formulated by the police authority, the criminal experts started the forensics analysis to figure out how the fraud has happened.

3. Forensic analysis

The first step in the forensic analyzes was the duplication of the hard drives. The hard drive was connected to a PC and a forensic version of a Linux distribution was used to boot the computer. The hard drives were duplicated using the dd tool. After the duplication, the hash values of the original and copies were calculated and compared to assure that the copy was a perfect bit by bit duplication of the original disks.

"(a) Perito Criminal - Instituto Geral de Perícias de Santa Catarina, wleitefilho@igp.sc.gov.br, Florianópolis, Brazil"

"(b) Perito Criminal - Instituto Geral de Perícias de Santa Catarina, romuloss@igp.sc.gov.br, Florianópolis, Brazil"

3.1. Searching the hard drive through regular expressions

A forensic analysis tool was used to analyze the images contents. The four images were mounted in a unique case and most of the automatic searches were done in all the four images at once.

The method used to look for the first evidence was to create several keywords using regular expressions. It was created keywords regarding banking activities, banking accounts, credit card numbers, federal taxes and others that would be related to the fraud in question.

The result of the regular expression search indicated some locations on the hard drive that should be analyzed more carefully. The evidences pointed by the search were on non allocated areas of the disk. A little data carving needed to be done to recover the original file structure that contained the data found. As the majority of the evidences found were text, this process occurred smoothly.

The first evidence found were pieces of electronic receipt of federal taxes related to the company that was also being investigated. The pieces of files were on the non allocated area of the hard drive and were recovered by the forensic analysis tool.

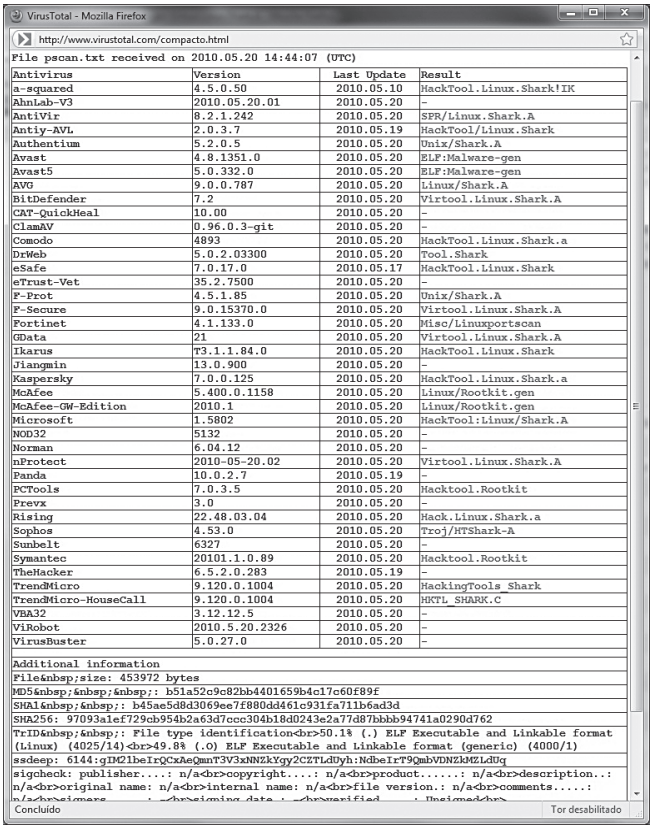
The figure 1 illustrates one of the taxes receipts recovered.

Comprovante de Pagamento
DARF
02 Permodo de Apuragco 31/01/2008
03 Nzmero do CPF ou CNPJ XXXXXXXXXXXXX
04 Csdigo da Receita 8109
05 Nzmero de Referjncia
01 Nome/Telefone
XXXXXXX CAPITAL - (259) 2040 06 Data de Vencimento 20/02/2008
07 Valor do Principal 9.528,64
ATENGCO
I vedado o recolhimento de tributos e contribuigues administrados pela Secretaria da Receita Federal cujo valor total seja inferior a R$ 10,00. Ocorrendo tal situagco, adicione esse valor ao tributo/contribuigco de mesmo csdigo de permodos subseq|entes, ati que o total seja igual ou superior a R$ 10,00. 08 Valor da Multa 0,00
09 Valor dos Juros e / ou
Encargos DL - 1025/69 0,00
10 Valor Total 9.528,64
11 Autenticagco Bancaria (somente nas 1* e 2* vias)
003412333956680
Documento aprovado pela IN/SRF - N: 81 de 27/12/1996.
O DARF - Documento de Arrecadagco de Receitas Federais acima foi pago atravis do Banco XXX Empresa. O langamento do valor consta no extrato da Conta Corrente, junto ` Agjncia do dibito N: 2X0X, da data de pagamento 18/02/2008, sob o N: de protocolo XX481XX.
Este documento serve como comprovante de pagamento e deve ser guardado para apresentagco ` Receita Federal, quando solicitado.
N: de Controle: 521683662508XXXXXX
Banco XXX S.A.
www.xxx.com.br
AUTENTICAGCO
PCSa7jWw IKmUmDsC j654*wog EPGJ9UZt zFtqRplh HD@uTI59 QOqRIpid PicbVbWA FpUG4rjH 5eGvpC7o iRt8Ca?b VXvguJ8z iXLdAQSK 63AwQs6b n@Jn#EcS *fC9Xlsh 3wv5gfOV Q*?EYs*V mAM6jtP2 UPwGMp?r GZoe2ngG kz?im@y? 84401660 08809220

Fig. 1. Electronic receipt found in the suspect computer

3.2. Scanning the hard drive with anti-virus software

One of the questions formulated by the police authority was about malicious code. The computers apprehended appeared to be used in hacking activities. The technique used to look for malicious code was to scan all the hard drives with anti-virus software. The anti-virus software pointed to a suspected code located in the Linux partitions of one of the hard drives. The piece of coded pointed by the anti-virus was submitted to the Virus Total [5], which is a service provided by the Web that submitted the sent file to the main anti-virus products. The results of the Virus Total are illustrated in the figure 2.


VirusTotal - Mozilla Firefox

http://www.virustotal.com/compacto.html

File pscan.txt received on 2010.05.20 14:44:07 (UTC)

Antivirus	Version	Last Update	Result
a-squared	4.5.0.50	2010.05.10	HackTool.Linux.Shark!IK
AhnLab-V3	2010.05.20.01	2010.05.20	-
AntiVir	8.2.1.242	2010.05.20	SPR/Linux.Shark.A
Antiy-AVL	2.0.3.7	2010.05.19	HackTool/Linux.Shark
Authentium	5.2.0.5	2010.05.20	Unix/Shark.A
Avast	4.8.1351.0	2010.05.20	ELF:Malware-gen
Avast5	5.0.332.0	2010.05.20	ELF:Malware-gen
AVG	9.0.0.787	2010.05.20	Linux/Shark.A
BitDefender	7.2	2010.05.20	Virtool.Linux.Shark.A
CAT-QuickHeal	10.00	2010.05.20	-
ClamAV	0.96.0.3-git	2010.05.20	-
Comodo	4893	2010.05.20	HackTool.Linux.Shark.a
DrWeb	5.0.2.03300	2010.05.20	Tool.Shark
eSafe	7.0.17.0	2010.05.17	HackTool.Linux.Shark
eTrust-Vet	35.2.7500	2010.05.20	-
F-Prot	4.5.1.85	2010.05.20	Unix/Shark.A
F-Secure	9.0.15370.0	2010.05.20	Virtool.Linux.Shark.A
Fortinet	4.1.133.0	2010.05.20	Misc/Linuxportscan
GData	21	2010.05.20	Virtool.Linux.Shark.A
Ikarus	T3.1.1.84.0	2010.05.20	HackTool.Linux.Shark
Jiangmin	13.0.900	2010.05.20	-
Kaspersky	7.0.0.125	2010.05.20	HackTool.Linux.Shark.a
McAfee	5.400.0.1158	2010.05.20	Linux/Rootkit.gen
McAfee-GW-Edition	2010.1	2010.05.20	Linux/Rootkit.gen
Microsoft	1.5802	2010.05.20	HackTool:Linux/Shark.A
NOD32	5132	2010.05.20	-
Norman	6.04.12	2010.05.20	-
nProtect	2010-05-20.02	2010.05.20	Virtool.Linux.Shark.A
Panda	10.0.2.7	2010.05.19	-
PCTools	7.0.3.5	2010.05.20	Hacktool.Rootkit
Prevx	3.0	2010.05.20	-
Rising	22.48.03.04	2010.05.20	Hack.Linux.Shark.a
Sophos	4.53.0	2010.05.20	Troj/HTShark-A
Sunbelt	6327	2010.05.20	-
Symantec	20101.1.0.89	2010.05.20	Hacktool.Rootkit
TheHacker	6.5.2.0.283	2010.05.19	-
TrendMicro	9.120.0.1004	2010.05.20	HackingTools_Shark
TrendMicro-HouseCall	9.120.0.1004	2010.05.20	HKTL_SHARK.C
VBA32	3.12.12.5	2010.05.20	-
ViRobot	2010.5.20.2326	2010.05.20	-
VirusBuster	5.0.27.0	2010.05.20	-

Additional information
File size: 453972 bytes
MD5   : b51a52c9c82bb4401659b4c17c60f89f
SHA1   : b45ae5d8d3069ee7f880dd461c931fa711b6ad3d
SHA256: 97093a1ef729eb954b2a63d7ccc304b18d0243e2a77d87bbbb94741a0290d762
TrID   : File type identification
50.1% (.) ELF Executable and Linkable format (Linux) (4025/14)
49.8% (.O) ELF Executable and Linkable format (generic) (4000/1)
ssdeep: 6144:gIM21beIrQCxAeQmnT3V3xNNZkYgy2CZTLdUyh:NdbeIrT9QmbVDNZkMZLdUq
sigcheck: publisher....: n/a
copyright....: n/a
product.....: n/a
description..: n/a
original name: n/a
internal name: n/a
file version.: n/a
comments.....:

Concluído Tor desabilitado

Fig. 2. Results of the virus total analysis

The Virus Total classified the malware as a Linux hacker tool. This malware is composed by a Linux executable file (ELF), some shell scripts, PHP files and other configuration tools. The criminal experts analyzed the source code of the PHP file and concluded that the malware was designed to perform a dictionary attack in e-mail servers. It was proved, by analyzing the Linux ".history" file, that the malware was executed. The source code, with commentaries added by the experts, is illustrated in the figure 3.

```
<?php
function POPa($username, $password, $server) {
$socket = fsockopen($server, 110); // POP3 port
    if (!$socket) {return "cracked";}
    $res = fgets($socket, 512);
    //reads  512 bytes, the expected result is the string "+OK"
    fputs($socket, "USER $username\r\n"); // send user name to the server
    $res = fgets($socket, 512); //reads more 512 bytes, expect "+OK"
    fputs($socket, "PASS $password\r\n");  //send user password to server
    $res = fgets($socket, 512); //reads more 512 bytes, expect "+OK"
    //at this point, the connection with the server was established, meaning that
    //the dictionary attack worked.
    fputs($socket, "QUIT\r\n"); //sends quit to the server
    fclose($socket); //close the connection with the server
    //at this point the attack worked, so it writes in the "vuln.txt" file the name
    //and password used to connect to the email server.
    $fp = fopen("vuln.txt", "a");
    fwrite($fp, " $server $username $password\r\n");
    fclose($fp);
     return "cracked";
}
//SET INITIAL LOAD
//The malware code execution starts HERE
$ip = $argv[1];  //receives as input parameter the IP address
 //READ USER/PASS FILE
//opens the dictionary file, with several names and passwords.
$fp = fopen("pass_file", "r");
$i = 1;
$c2= 1;
//run until the end of "pass_file"
while (!feof($fp)) {
    //reads user name and password, line by line
    $propozitie = fgets($fp, 4096);
    $propozitie = explode(" ", $propozitie);
    $user[$i] = $propozitie[0];
    @$pass[$i] = $propozitie[1];
    $i = $i + 1;
    $c2 = $c2 + 1;
}
fclose($fp); //close "pass_file"
//Do BRUTE-FORCE ATACK
$x = 1;
$chestie = "not";
//runs until the end of the user/password list or until the attack has worked
while (( $x < $c2 ) and ( $chestie != "cracked" )) {
    //call POPa functions, informing user, password and IP.
    $chestie = POPa($user[$x], $pass[$x], $ip);
    if ( $chestie == "cracked" ) {
    $quit = 1;
    }  //if
    $x = $x + 1;
}
//End of malware script
?>
```

Fig. 3. PHP malware

Although it could be proved that the malware was executed, there is no evidence that the attack worked. The "vuln.txt" file that was supposed to have the results of the attack was empty.

The malware pointed out the suspect used to practice hacking activities and had some degree of computational knowledge. This information would be enough to answer one of the police authority question about malware software. But no evidence was found that indicated a direct relationship between this attack and the banking fraud in question. It became clear that more research would be necessary.

3.3. Looking for e-mail data

The next step in the forensic analysis was to look for e-mail data. E-mails files have a specific signature. Accordingly Tanenbaum [2], a basic e-mail file format is specified by the RFC 822, which defines the e-mail as ASCII characters structured in a primitive envelop with some header fields, a blank line and the message body. Each header field is composed by a name, a colon mark and a value. The main fields of the header are: "To:", "Cc:", "Bcc", "From:", "Sender:", "Received:", "Return-Path:", "Subject:" etc. The RFC 822 mentions that the users can create new header fields, since they start with the string "X-". The evolution of the RFC 822 is a standard know as MIME (Multipurpose Internet Mail Extensions). The idea of MIME is to use the RFC 822, but add structure in the message body and define rules that other types besides ASCII code can be sent. With MIME, non English alphabet can be sent, multimedia data and others types of information. The MIME defines the following header fields: "MIME-Version:", "Content-Description:", "Content-Id:", "Content-Transfer-Encoding:" and "Content-Type:".

The e-mails information may be stored on non allocated areas of the hard drives or in temporary internet files. It's important to known how the e-mail data is structured, so the entire hard drives can be searched to find e-mails signatures.

This search was automated by the forensic analysis tool. The tool reported several data that matched e-mails signatures. Each one was closely analyzed by the criminal experts. At the "InBox.dbx" file it was found several e-mails related with the Bank Institution that was victim of the fraud. The e-mail is presented in its HTML form at figure 4.

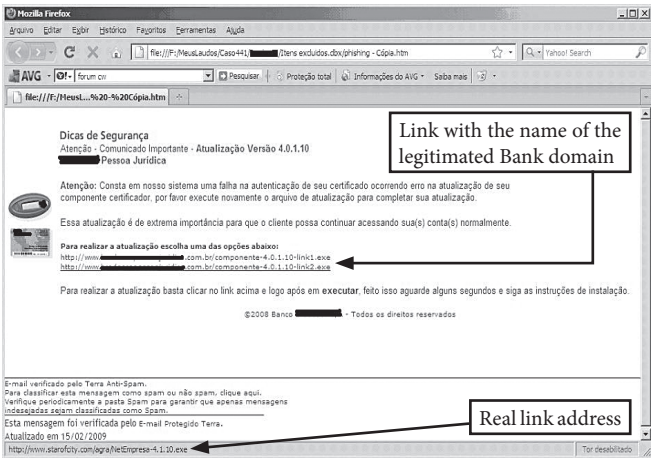


Fig. 4. Phishing E-mail

This e-mail is a classic phishing attack. It requests the user to click in its links to update a security banking software and advise the user to do so, otherwise new banking transaction will not be possible. The link exhibited in the e-mail body shows the real bank domain, but at the bottom of the Web browser it's possible to see that the user will be redirected to a different domain.

This phishing e-mail linked the suspect with malicious activities related to the victim Bank.

At this point, solid evidence has been found against the suspect, but we believed more data could be found. Luckily,

one of the phishing e-mail link was not broken. The malware code (NetEmpresa-4.1.10.exe) could be downloaded from the malicious Web site and executed in a controlled environment at the Computer Lab. The procedures and results of this analysis are described in the following section.

4. Malware analysis

Skoudis [8] defines the malware as a set of instructions that run on your computer and make your system do something that an attacker wants it to do. Accordingly to him, malicious code running on a computer could do any of the following: delete sensitive data; infect the computer and spread itself to others computers; monitor keystrokes and let an attacker see everything it's typed; gather personal information, computing habits, the Web sites visited; send streaming video from the user computer and remotely look over the user's shoulder; execute attacker's commands; etc. The possibilities are truly endless and depend on the attacker's creativity.

Skoudis [8] discuss a lab architecture based on virtual machines to analyze malware. At this environment it's possible to run different operation systems simultaneously on a single hardware box. Another advantage of using virtualization to test the malware is the possibility to easily roll back any changes to a virtual machine without rebuilding a system, immediately restoring a guest operating system to its original configuration.

To test the malware downloaded, a VMWare Server 1.10 virtual machine was created. In this VM, the Windows XP operational system was installed. The VM Ethernet interface was configured as "host only". This configuration prevents any access from the malwares to networks outside the VM environment. This measure prevented the malware to cause any damage in the external systems. After the OS has been installed and the Ethernet cable has been configured, the Wireshark [7] packet capture software was installed. It was expected that the malware would capture some user data and try to send them through the Internet. With the packet capturing activated the criminal experts could monitor the malware behavior. Finally, some tools from the sysinternal [3] [9] collection tools were installed to monitor the malware process activity.

With the environment ready, the malware NetEmpresa-4.1.10.exe was executed. The first screen presented by the malware used the name and logotype of the victim bank, informed the user that a certification component was going to be installed and alerted the user that she must be connected to the Internet (figure 5). The second screen (figure 6) asked the user to enter the token number that is provided by the bank. After the token number has been entered, the malware reported an error and asked the user to enter the token number again. This process was repeated for five times. After that, the malware finished execution.

After this first attempt, the packets captured were analyzed. It could be seen that the malware tried to establish an SMTP connection with an e-mail server located at smtp.terra.com.br. This connection could not be established because there was no e-mail server available in the VM environment.

The next step was to create a new VMWare machine and provide a SMTP service at this machine, supplying the malware with the service that it was trying to use.

At this point, the criminal experts did a short research about the SMTP protocol. Accordingly Tanenbaum [2], the SMTP is a very simple ASCII protocol that establishes a TCP connection in the port 25. After the connection in the port 25 is established, the client's computer waits until the server starts the communication. The server starts sending a text line that provides its identity and informs that it's ready to receive messages. In case the server is not ready, the client will end the connection and try again later. If the server is ready to receive messages, the client will inform from whom the message comes from and to whom it will be sent. If the receipt of the message exists at the message destination, the server will send the client a signal asking it to send the message. The client will send the message to server and the server will acknowledge it. It's not necessary any check sum, because the TCP provides trustfully communication. The main SMTP server messages are "220 xyz.com …", "250 xyz.com say hello …", "354 Send Mail", "250 Message accepted" and "221 xyz.com closing connection".

Based on this information, the criminal experts created a new VMWare machine and installed a Linux distribution on it. The distribution chosen was BackTrack 4 [6]. This distribution is set to penetration tests and some forensic activities. Because the SMTP is a vey simple protocol, the e-mail server was simulated using the Linux netcat tool and the server SMPT messages were send one by one entering them in the netcat console. This approach seemed more efficient than install and configures a real e-mail server.

The virtual machine with Linux was started and the netcat tool was launched to listen at port 25. The malware was executed again and the network packet traffic captured (figure 7).

The malware established a connection with the Linux machine at port 25 and started communication using the SMTP protocol. As the malware, working as a client e-mail, sent the messages, the proper requests were typed in the netcat console. This technique allowed the malware to complete the connection and sent all the data it was supposed to send. The malware client messages were received and registered by the netcat tool. These messages formed the e-mails showed in the figure 8.

The malware worked starting to send a first e-mail with the information "+ alert +". A second message was sent, with the information "++ info" and the first user's security data captured. Four more messages followed, with the data "-1", "-2", "-3", "-4" and four new user's security data, respectively.

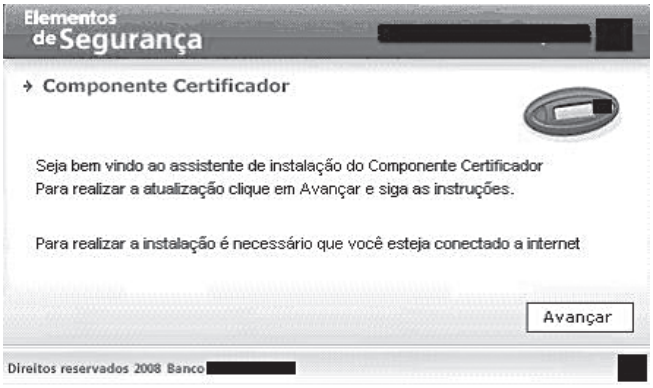


Fig. 5. Screen 1 of the Malware

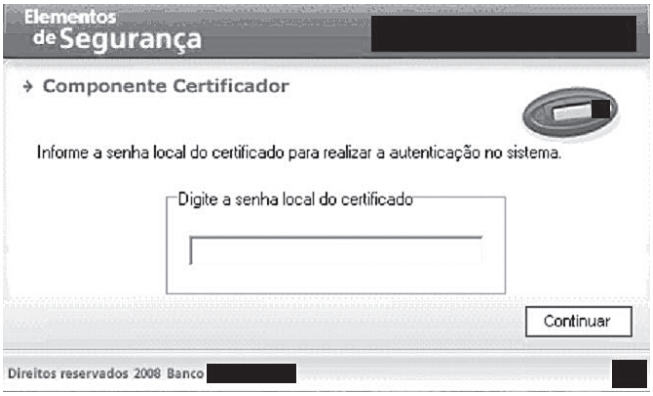


Fig. 6. Screen 2 of the Malware

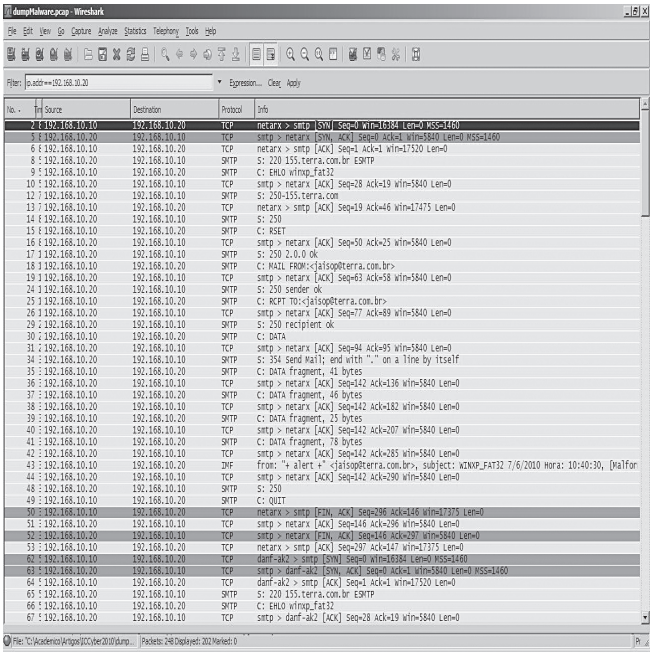


Fig. 7. Network dump for Malware activities

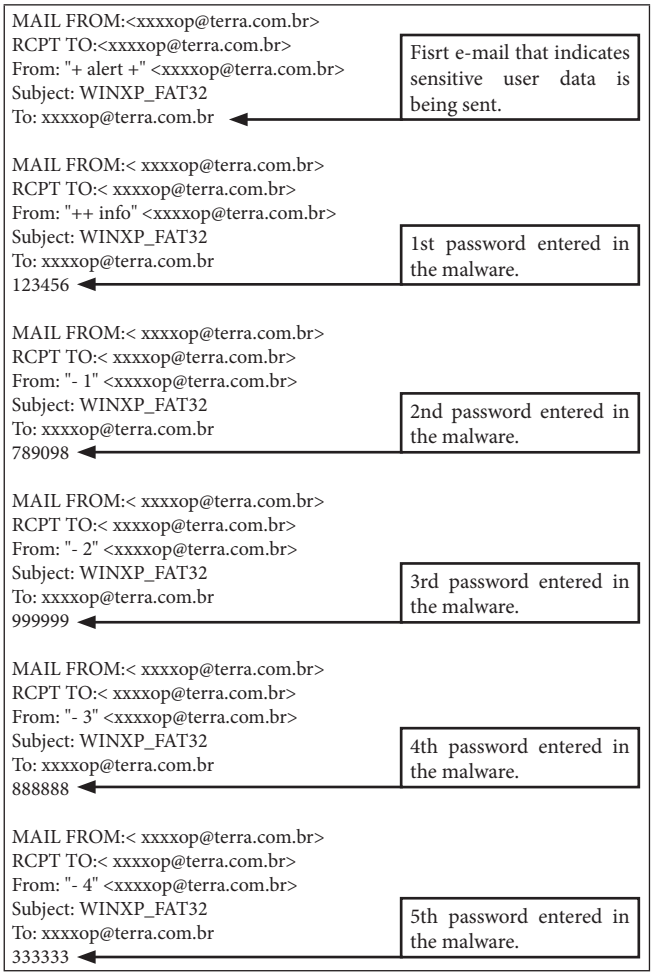


Fig. 8. E-mails sent by the Malware

Once the malware behavior and artifacts were discovered, a new search for e-mails that would be compliant with the ones sent by the malware tested was performed. It was found, at the "Excluded Items.dbx" file, several e-mails with the same characteristics and structure of the e-mails sent by the malware at the laboratory. This evidence proved that the malware was executed and e-mails with users' security data were sent to the suspect's computers.

5. Conclusion

In this article, a forensic analysis of real Internet banking fraud was presented. Based on the material received at Crime Lab and the information presented by the victims to the police force, the criminal experts used some search and malware analysis techniques to look for evidence. The evidences found could relate the money improperly transferred from bank users' accounts to the suspect's computers apprehended.

Putting all the pieces together, it was proved that the suspect had some computer crime knowledge and effectively performed successfully criminal actions against the victims. The criminal experts report provided the necessary information that the justice needed to prosecute the offender.

Acknowledgements

The authors would like to acknowledge the Criminal Expert Ana Carolina Ferrari that had patience to review this paper and provided us with useful suggestions and comments.

References

[1] Howard, Richard et.al – Cyber Fraud Trends and Mitigation – In The International Journal of Forensic Computer Science - Cyber Crime Investigation (ICCyber'2008) – Departamento de Polícia Federal, Rio de Janeiro: 2008

[2] Tanenbaum, Andrew S., "Redes de Computadores", Tradução 4.a Edição – Rio de Janeiro: 2003

[3] Russinovich, Mark E.; Solomon, David A. – Windows Internals 5th Edition – USA: 2009

[4] http://en.wikipedia.org/wiki/Phishing - accessed in 27th June, 2010.

[5] http://www.virustotal.com - accessed in 29th June, 2010.

[6] http://www.backtrack-linux.org/ - accessed in 2nd July, 2010.

[7] http://www.wireshark.org/ - accessed in 2nd July, 2010.

[8] Skoudis, Ed., Malware – Fighting Malicious Code – USA: 2004

[9] http://technet.microsoft.com/pt-br/sysinternals/default.aspx - accessed in 10th July, 2010.

Wilson Leite da Silva Filho holds a bachelor degree in System Information, a specialization degree in Information Security by Instituto Tecnológico de Aeronáutica (ITA, 2008) and a master degree in Computer Engineering by Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT/USP, 2005). Nowadays, he is Criminal Expert at Instituto Geral de Perícias do Estado de Santa Catarina (IGP/SC). He had already worked as Network Security Specialist at Companhia de Processamento de Dados do Estado de São Paulo (PRODESP) in 2008 and as Senior Software Engineering at Diebold Procomp, from 1999 to 2008.

Romulo Soares da Silva is a systems analyst with over 10 years of experience in programming, systems architecture and database administration. He has several courses in programming and database administration. He has worked with government tax systems of Florianópolis and São José cities. Nowadays, he is Criminal Expert at Instituto Geral de Perícias do Estado de Santa Catarina (IGP/SC).