International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 02 | May-2015 www.irjet.net p-ISSN: 2395-0072

Collecting Digital Evidence: Internet Banking Fraud - Case study

P.S. Lokhande[1]; Dr. B.B. Meshram[2]

[1] Asst. Professor, Dept. of Computer Engineering, AIKTC, Maharashtra, India
[2] Professor, Dept. of Computer Engineering, VJTI, Maharashtra, India

---

Abstract - ***Net banking frauds are now a day's became*** *common, criminals use the various available technologies to con the unaware citizens. Use of Phishing mails, key loggers and mobile phone SIM card cloning is the techniques commonly used. Highest number of Cyber Crimes made the job of police department tough. Tracing the non history shitter criminals, is an another challenge. Various online resource such as anonymizers equip criminals with loads of facility*

Key Words: Phishing, Net banking fraud, Hacking, Digital Evidence, Mobile SIM cloning.

1. INTRODUCTION

Case Story- Fund transfer (Union Bank) Airoli, Navimumbai: Someone has hacked the password of net banking and siphoned Rs. 4 Lac 60 thousand. Case of net banking account hacking and theft is registered at Rabale, Navimumbai Police station. A case has been filed under various sections of IPC- Indian Penal Code[1] and ITA 2008[2] acts.

A) Indian Penal Code sections 34 (common intention),
B) 120-B (punishment for criminal conspiracy) and 420 (cheating), and
C) IT Act sections 65 (tampering with computer source documents),
D) 66-B (dishonestly receiving stolen computer resources),
E) 66-C (identity theft)
F) 66-D (cheating by impersonation by using computer resource).

Fabrication unit in Rabale MIDC have current account with Union Bank, Airoli Branch. Mainly this account was used for the purpose for paying online sales tax, advance tax and income tax to government.

1.1 Crime Registered

Rabale Police Station, Rabale, Thane Belepur Road, Navimumbai, Maharashtra, India

2. HISTORY OF EVENTS

Event flow: On Friday evening victim got the SMS message from bank that you added Mr Tewari (Name changed) as a beneficiary for the transfer of payment through net banking and to approve that please login to the account and enter the verification code received on victims mobile. Victim ignored that SMS considering usual SMS's from bank. Saturday morning he got the sms message from the bank that beneficiary Mr Tiwari added successfully, upon receiving this message he ranged bank but unfortunately hackers particularly selected the day when bank is off on Saturday (26th Jan) and Sunday. Victims repeated attempts to call bank went in vain. After 24 hours of adding beneficiary hacker initiated the fund transfer and transferred Rs. 4.60 lac to his account in standard chartered bank.

2.1 Possible Techniques used by the hacker:

i) Password Cracking for getting in to the net banking.
ii)Possible method used to steal the password.
iii) Spam mail found on victims computer look like of union bank mail redirecting user to the spoofed page of union bank asking information of user such as User id, password and transaction password.

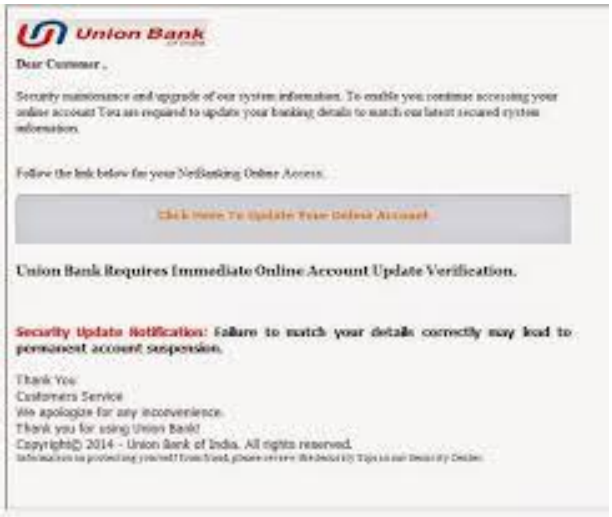

Fig. 1 Screen shot of email : Pretend to be sent by Union Bank

iv) Hacker might have Placed keylogger in victim's pc from where he recorded net banking password as well as transaction password [6].
v) Cloned the SIM card of victim's mobile number.

2.2 Steps in SIM card Cloning:

What is SIM card cloning? In simple words we can define Sim Card cloning as "*It is the process of cloning a original*

SIM card to create another duplicate SIM card without the knowledge of individual mobile subscriber (which is illegal)"[3][4].

Steps in SIM cloning:

a) Scan the SIM to extract IMSI and Ki, the 128 bit key.
b) Put the IMSI and Ki into some card Software
c) And then copy it into a new SIM card

2.2.1 Possible cloning method used by the hacker with the help of tools such as

a) Simscan from Dejans
b) KiSsMi
c) Mobiledit

Screen shot of the SIM cloning software and hardware device.

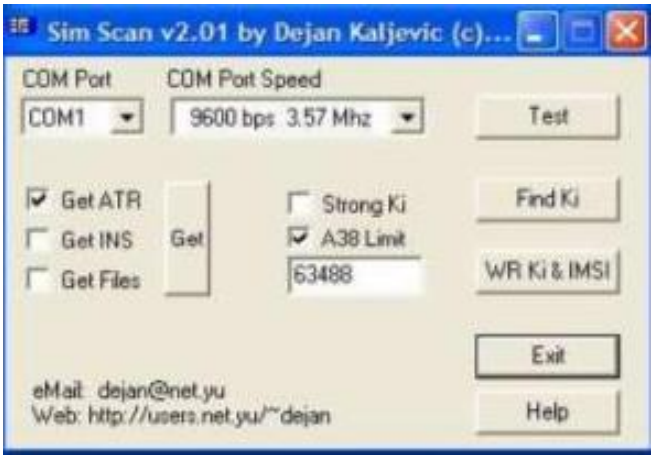

Fig 2. Sim Scan software.

Fig-3. Simcard Cloning hardware device

4) Used 5 different mobile phones to access the internet.
5) One of the transaction traced by us is from Hong Kong server, possibility that hacker may have used anonymizers to mislead the investigating team.

Example of online Annoymizers:

i) http://online-anonymizer.com/
ii) https://www.anonymizer.com/
iii) https://www.hidemyass.com/

3. Challenges faced by Law and Enforcement Agency

i) No formal technical knowledge on how to deal with the internet fraud cases.
ii) Struggling to establish the chain of evidence, as there is no visible evidence to start with.
iii)Lack of Cyber forensic knowledge
iv) How to setup the action plan for investigation.

3.1 Methodology Adopted to Collect the Digital Evidence.

i) Made an initial assessment about the type of case.
ii) Victim got the sms first : we searched the trigger for the sms server from the server log, which came from the Union bank main server. Notifying addition of beneficiaries in net banking account.
iii) Searched the log of the main net banking server for the server log for recording the event for the victims userid, we found the IP address from where the account is logged in for adding of beneficiaries found IP : 199.58.84.31, we believe that hacker used the annoymizer to spoof the original IP
iv)Based on the received IP address we traced its location with the help of various ip tracing tools , such as"what is my IP.com" and traced it to Hongkong location belongs to Hongkong TV media company.

Screen shot of the website providing the ip tracing utility.

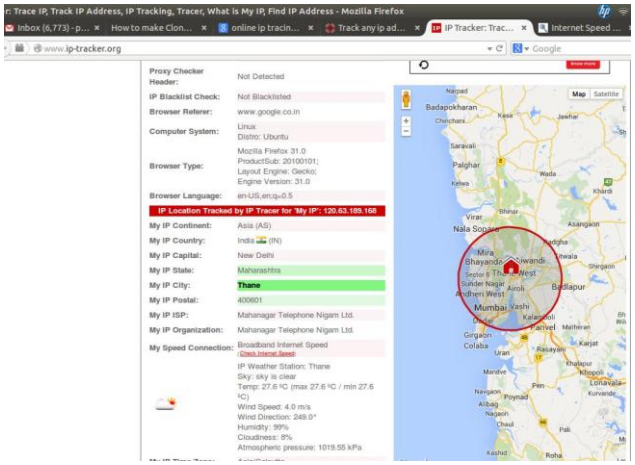

Fig-4. www.ip-tracker.com website [4]

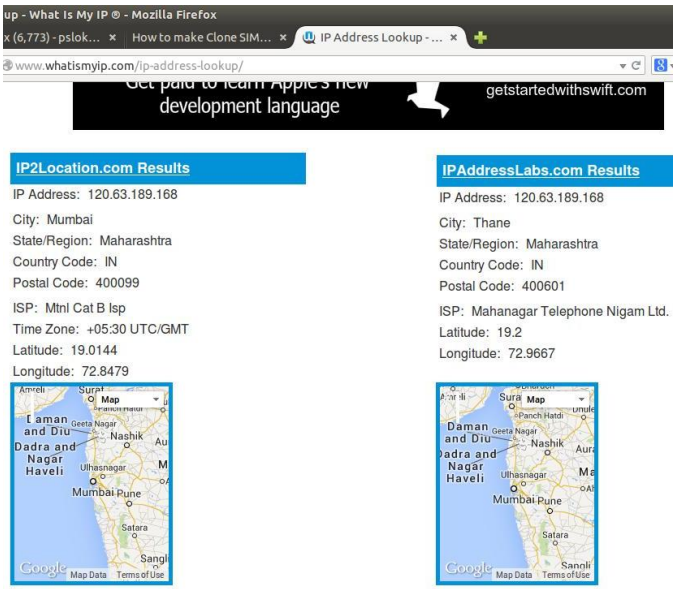

Fig-5. : www.whatismyip.com website

IP address 199.58.84.31 kept on monitoring on "monitis" (www.monitis.com) [7]

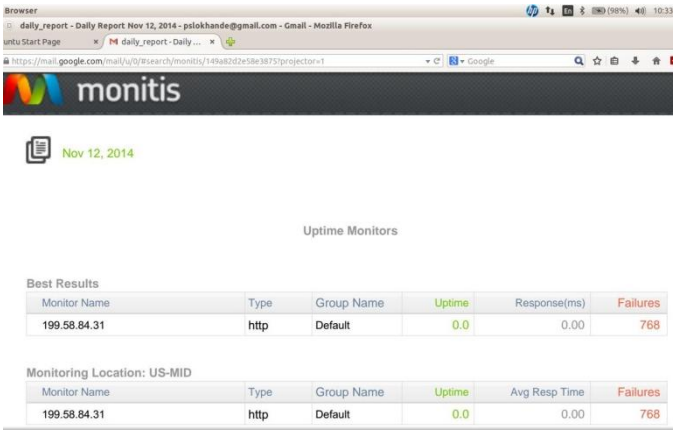

Fig-5. Daily uptime monitors through various servers on monitis.com

Determining preliminary design or approach to the case.
Chain of events table : used to systemically list the event flow with respect to time and person.

Table -1: Chain of Crime Events

Event No	Source (Person, Computer, device etc)	Medium (paper, phone, electronic etc)	Destination (Person, place, organization)	Impact / Incident	Date	Time	Place

Chain of custody table : At the time of collecting evidence, there is a need to have the listing of confiscated items with their identity i.e serial number

Table -2 : Chain of custody.

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Created detailed design for the investigation listed as follows.
- Location based on IP address
- Fund transferred to Standard chartered bank:- details of account holder with address proof and photograph.
-CCTV images of the ATM from where criminal withdrawals amount.
- Mobile phone number as per the standard chartered bank
- Mobile phone number through which the internet is accessed and its CDR records (Mobile tower location data)

4. Methodology Followed to collect Digital Evidence.

Digital evidence is fragile and can be easily destroyed or rendered inadmissible in court due to modification after it is collected. IT incident response teams need to recognize that, if an intrusion or attack has a chance of ending up in criminal prosecution, evidence handling is crucial to winning the case and bringing the criminal to justice [5]

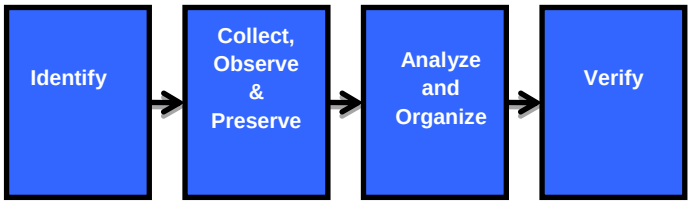

Fig-6 Methodology for collection of Digital Evidence

i) Identify: Any digital information or artifacts that can be used as evidence.
ii) Collect, observe and preserve the evidence
Iii) Analyze, identify and organize the evidence.
Iv) Rebuild the evidence or repeat a situation to verify the same results every time. Checking the hash value.

4.1 Information required: to establish the chain of custody

i) Who added the beneficiary Mr Tiwari through net banking account? What is the time of request and IP address from where the request is initiated?

ii) Who confirmed the added beneficiary? (Net banking is having the process of confirming the added beneficiary in net banking by entering the confirmation code received on mobile phone). We suspect that fraudster cloned the SIM of victim.
iii) IP address of the system from where the fund is transferred.
iv)Details of the beneficiary account, where the fund is illegally transferred from victims account.
v) Based on the detail in bank and mobile number, get the details of Mobile activity i.e. location call details.
vii)Details of ATM and Bank from where the fund is withdrawal, CCTV footage

We started with the given inputs from the victim and contacted bank IT division to get the server log to trace the location of fraudster.

4.2 Evidence Collected.

i) IP Address of system from where the beneficiary add request is initiated: We traced the IP address and found that the IP address belongs to the Hong Kong Company. This is just to misguide the law and enforcement agency. As we suspect that fraudster used Anonymizers to spoof the IP.
ii)Collected the data from the beneficiary bank account (Standard Chartered Bank) Lucknow, UP branch. Later we checked with the mobile service provided where we found the 5 different numbers were taken on the five different addresses and identity proofs.
iii)Identified the IP address of device from where the actual fund is transferred, we came to know that internet is accessed from mobile phone, we traced down the location to Agra Railway station. Fraudster used different mobile phone to access the internet having no call records
iv)Collected the CCTV footage of Standard Chartered bank ATM from where the fraudster withdrawals the money. Based on the footage the we zeroed down on a particular name of person (footage is compared with 5 different mobile numbers with five different addresses and identity proofs. We succeeded to match with one.
v)Matched number was kept on the surveillance; fraudster is continuously changing his location.
vi)Fraudster purchased Jewelry worth Rs 1 Lac 90 thousand from a jewelry shop from Allahabad. Police initiated seizing process of CCTV footage of jewelry shop.
vii)Upon confirming his identity (Bank ATM footage, Jewelry shop Footage and ID proof photo) police party was sent to arrest him.

4.3 Preservation of Evidence.

- Preserved the server log of Union bank and Standard Chartered Bank.
- Preserved the Mobile tower location CDR data
- Preserved videos from the original source the CCTV footage data (Standard Chartered Bank, ATM, Jewellery shop)

4.4 Analysis and Verification:

Preserved Evidence is then sent for the analysis and verification to concern competent authority.

5.CONCLUSION

Cyber crimes are very common and criminals are using very sophisticated tools to commit the crime such as Mobile SIM morphing, Anonymizers, Phishing mail, Nigerian Fund Transfer fraud etc. Various hacking websites offering number of hijackings software tools. Cyber criminals are taking advantage of peoples having less awareness about the Spam messages, Phishing mails from where they can steal the required information. There is a need to track such activities by incorporating the SPAM filter, Phishing filter in web browser itself. Also banking organizations should take the step forward to educate the user, make them aware about the probable threats to his money through net banking.

6. REFERENCES.

[1] Indian Penal Code : http://www.ipc.in/
[2] Indian IT ACT 2000 : http://www.dot.gov.in/act-rules/information-technology-act-2000
[3] http://www.87android.com/what-is-sim-card-cloning/#ixzz3alOPfA00
[4] Svein Yngvar Willasse, "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence, Spring 2003, Volume 2, Issue 1
[5] IP Tracker website : www.ip-tracker.com
[6] P. S. Lokhande, B. B. Meshram; "Learning from Past Intrusion Attacks: Digital Evidence Collection to Make E-commerce Systems more secure", ICL2009,ICL 2009 Proceedings,September 23-25 , 2009 Villach, Austria, Page 824-826,2009
[7] P. S. Lokhande, B. B. Meshram, "Botnet: Understanding Behavior, Life Cycle Events & Actions", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 4, Issue 3, Pg.36-42.,Mar-2014
[8] http://www.monitis.com/ : All-in-one application monitoring platform

ACKNOWLEDGMENTS

Our sincere thanks to the Rabale Police Station and its officials, Rabale, Navimumbai, State Maharashtra, India, who have provided access to the case to work on it.

BIOGRAPHIES

P.S. Lokhande is working as Assistant Professor in Computer Engg. Department, Kalsekar Tech Campus, Navimumbai, University of Mumbai. He has 15 years of teaching experience. Published more than 25 research papers in reputed conferences and International Journals.

B.B. Meshram is working as Professor in Computer Engineering department in VJTI, Matunga, Mumbai. He has more than 25 years of teaching experience. He has guided number of Masters and PhD students. There are two patents in his credit in the field of Computer Engineering. Has published more than 100 research papers in reputed conferences and International Journals.

