International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Forensic Analysis Overview of Banking System Malware

Dnyandev Najan[1], Rajendra N Kokare[2], Vishal Pawade[3], Dr. Krishna Kulkarni[4]

[1]Ex-Scientific officer, Regional Forensic Science Laboratory, Government of Maharashtra, Ganeshkhind, Opp. Rajbhavan, Pune-411007
[2]Deputy Director, Regional Forensic Science Laboratory, Government of Maharashtra, Ganeshkhind, Opp. Rajbhavan, Pune-411007
[3]Asst Director, Directorate of Forensic Science Laboratory, Government of Maharashtra, Kalina, Santacruz East, Mumbai-400098
[4]Director, Directorate of Forensic Science Laboratory, Government of Maharashtra, Kalina, Santacruz East, Mumbai-400098
dnyandev.najan[at]gmail.com, dydir.rfslpune[at]maharashtra.gov.in, vishal.pawade24[at]gov.in, dir.fsl[at]maharashtra.gov.in

Abstract: ***Now a days Online banking uses advanced digital technology. It has given the society an advantage as it saves the time and reduce the human effort. At the same time, there are some risk factors that are associated with this extensive implementation of technology. One of them is malware attack. Attackers use the malware to compromise the Banking Systems and other target system. Malware is nothing but the malfunction program which is coded as per the attacker's convenient trap. Malware in banking systems make big financial loss to the Economy. In this paper we have described the cases which were successfully analyzed and reported using EnCase - ThreadGrid and open source tools like Autopsy. We are emphasizing the use of some lesser known methods of Malware detection using EnCase Guidance Software.***

Keywords: Cyber Forensics, Forensics tools – open source, Malware, ATM, Banking System, SWIFT, IT Security

1. Introduction

MALWARE in computer hacking is the vital tool for hackers. To crack or compromise the regular activity some malfunction programs run by attackers for financial income or some other intentional purpose. Indirectly they commit the crime. Here are the regular process of banking system and ATM transactions.

There have vendors present in between the bank and customers. When any person access ATM machine to withdraw money there are two possible cases of transaction procedure. First one is the customer using same bank ATM machine and another case is customer using other bank's ATM machine for transactions. Both cases have different authentication layers. Generally using other bank ATM machine will go through multiple authentication and flow compared to bank customer using same bank's ATM machine.

There are servers that work in coordination for the smooth and secure working of ATM and SWIFT fund transfers. There are specialized hardware and software applications used for the online security of these transactions. ATM authentication server and SWIFT server were compromised using malwares which skipped the authentication process of ATM transactions and money transfer using SWIFT accounts. Malware analysis can be done in two ways, static and dynamic. There are several challenges in Malware analysis. Anti-Forensic tools are one of the biggest challenges faced in Malware forensic analysis.

2. Banking transactions

Automatic teller machine (ATM) allows you to do the banking transaction without bank representative from anywhere where ATM machines are located. Once the card holder inserts the card in ATM machine and enter the required details, the details are verified from bank servers. In following block diagram Figure 2, it shows the working of ATM internal structure.

Another method for banking transaction includes Online banking/internet banking, SWIFT transaction. We tried to explain about the ATM transaction, SWIFT fund transfer and normal internet banking. First of all, general ATM internal structure or block diagram of ATM mentioned in Figure 1. Attackers try to find the loop holes in routine procedure or in system and then select the target for attack. To complete the Forensic analysis in banking sector there is big need to understand the whole structure and working of banking elements. Nowadays IT security is very crucial and can be achieved by using updated techniques and technologies.

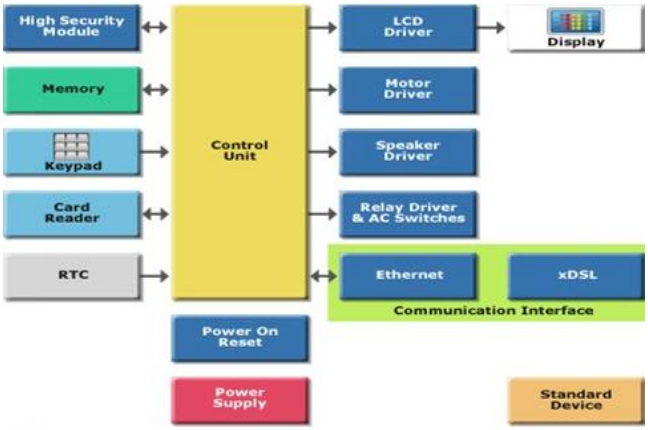


Figure 1: ATM Block Diagram

ATM Networking:
ISP-Internet service provider plays very important role. They provide communication between ATM (Automatic teller machine) and host processors. For a successful transaction,

the card holder needs to enter required information like Account type, Pin etc. The entire information is then passed on to the host processors which check the details with authorized bank.

There have two types of ATM Machine first one is leased line ATM Machines and second one is Dial-up ATM machine.

i) Leased Line ATM Machine: Maintenance and operating facility of these machines are higher than dial-up. Leased line machine /system are connected directly to the host processor through four wire point to point dedicated telephone line.
ii) Dial-up ATM Machine: The Dial-Up Machines connect to the host processor through a normal phone line using modem. This requires normal connection. Installation and cost of the Dial-up ATM machine is very less compared to leased line ATM Machine.

X Bank -> X ATM:

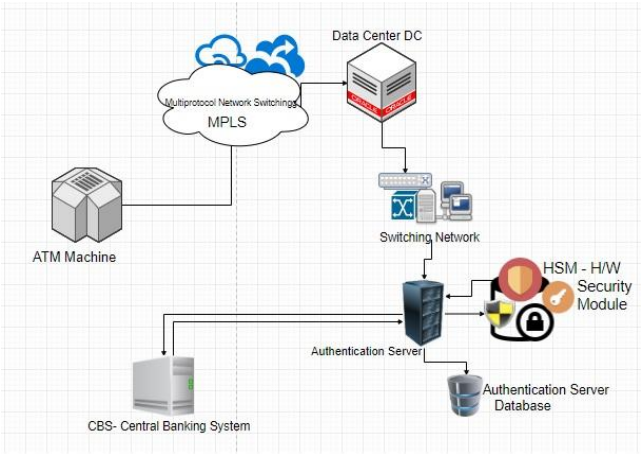


Figure 2: Transaction request from Bank's ATM

X Bank -> Y ATM:

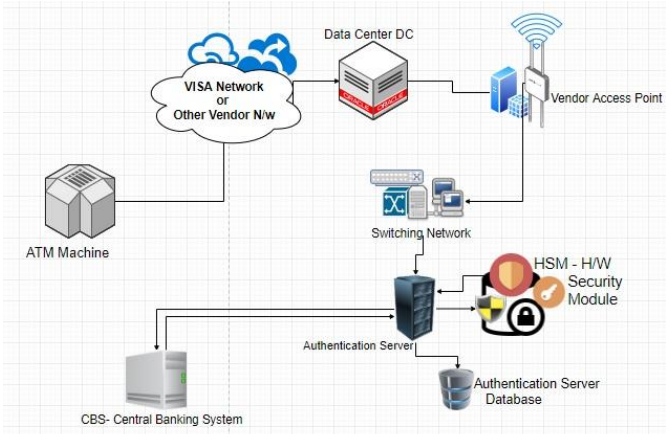


Figure 3: Transaction request from different Bank's ATM

Banks uses different technologies to transfer money within country or globally. Block-chain technology is better than SWIFT transfer and it can replace the SWFIT transfer for secure transaction. In SWIFT, there are checker and maker. Checker and maker create the SWIFT message with proper authority. After SWIFT message generation the next process takes place which is approval. For approval purpose, authentication request gets redirected to main SWIFT management server which is located in Belgium. Worldwide SWIFT transaction is managed by the main SWIFT server located in Belgium.

Banks have their specific checker and maker at branch or in headquarters of bank. After all SWIFT messages were get approved by the higher authority (Checker and Makers) of bank. Generally, the messages are fully encrypted for security purpose. Even if checkers and maker's system gets compromised, there is second level of security to check the transactions. With acknowledgement by higher authority of bank, transaction get completed.

SWIFT transaction in Banking:

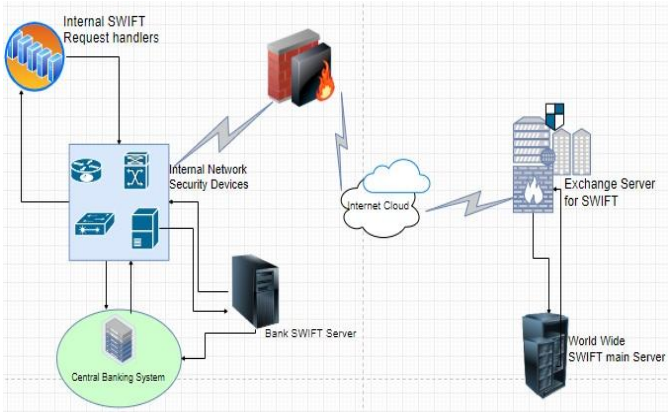


Figure 4: SWIFT Transactions

3. Brief History of Case

XYZ bank chairperson and team got alert that there was huge transaction from bank in weekends. They checked in banking system and noticed that there was unauthorized transaction from bank.

As per the Information Technology (Intermediaries Guidelines) rules 2011 it is obligatory on the part of banks to report cyber security incidents to the Computer Emergency Response Team-In (CERT-In). After reporting CERT-In they visited the crime scene and completed the standard procedure from there end. Bank filed a complaint against unknown person. As per the IT act complain was registered immediately under IT act [6] and Police department took help from forensic science laboratory, Pune and visited crime scene. Unauthorized transaction was taking place in two ways, one in ATM cash withdrawal and another in SWIFT transfer. After comparing the normal working structure of bank with the working of bank system after compromise, forensic team acquired suspicious server images and other local system images. Some systems were located in bank branch. All suspected devices were seized in forensically sound manner by police officials under the guidance of forensic laboratory team.

The traces of unauthorized transaction were captured from banking applications and web-based application.

4. Forensic Investigation

Forensics team when visited the crime scene (bank) identified that the suspicious infected servers and systems were in ―switch-on‖ mode but were disconnected from internet connection line as per the instruction from CERT-In team. Most servers were located in Virtual environment. The Forensic team conducted the investigation in two steps [5]: Collection of digital evidence and Analysis of collected digital evidence.

Step 1-Collection of digital evidence from bank: Forensic team acquired twelve server images, all of them were in virtual environment. Using FTK imager forensic team performed Imaging of suspected servers and systems. After accessing the access point of virtual machine, we acquired all required suspected servers' images. Those images were saved in access point server and then gathered all images in storage devices.

Forensic team also collected the footage of CCTV, network connection details, log files of network devices such as SIEM logs, Firewall Logs, etc., internal structure of banking system, Intranet & internet application details of bank, third party application list, whitelisted application, user details and other bank details also collected for analytics.

Step 2 -Analysis of digital evidence: Captured images were having different operating system platform. The operating system platform used by bank was windows version, Linux, AIX (IBM Customized operating system).

Data from Applications: Configuration setting of applications, Logs, application and network architecture, Exchange Server, E-Mails, Web uses, Data/File Sharing, Security Applications were collected. Compared white listed email IDs and IP addresses and suspected the Phishing emails.

Using data from Data collection: Collected files and E01 images of SWIFT server. Extracted data for analysis. Forensics analysis on Event logs and System logs indicated the suspected execution files. The traces of files were recovered from the slack spaces and Unallocated spaces using data carving. Hence forth used multiple forensics tools including commercial and open source.

Data from Volatile and Non-Volatile: Due to the lack of knowledge on forensics and incident response process internal staff couldn't stop the deletion of virtual machine which created by attacker. Hibernation files and network captured data were analyzed which were revealed the suspicious script and dependent suspicious execution files. Maximum data were recovered from the non-volatile data.

Data from Network Traffic: Source and destination IP addresses listed including IP protocol number. Firewall, routers, IDS and IPS logs filtered using recent use cases. The past attack on bank system matches with the current bank cyber-attack.

After all possible way of analysis following findings and traces were noted.

5. Findings & Traces

1) Risky setup files were found in SWIFT server. [FileZilla_3.35.1_win64-setup_bundled_[CLIENT].exe, FileZilla_Server-0_9_60_2_[SERVER].exe and FileZilla_3.17.0.1_win64-setup.exe] which enable FTP access to target system.
2) PowerShell execution policy found enabled on SWIFT Server.
3) Traces of malicious executable files were found in SWIFT Server in %systemdrive%\PrefLogs. References: -tb.ps1, sqloper.exe, pmon.exe, appsrv mdtdt.exe and r.bat.

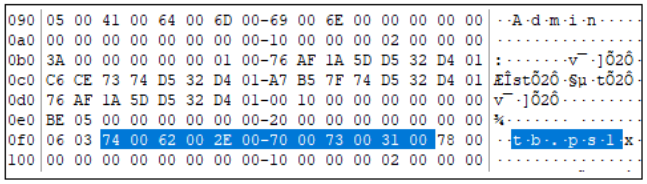


Figure 5: tb.ps1x file trace

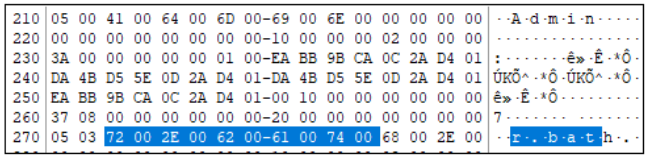
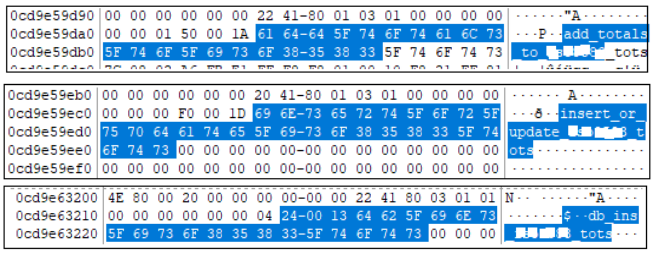


Figure 6: r.bat trace

4) Logs of suspicious transfer were found during of bank hacking incident.
5) Compromised ID logs were included in suspicious transaction, FTP-Admin User IDs DEB and other accounts.
6) People who left/resigned from bank 6 month before still their login credentials exist in AD.
7) Traces and Phishing emails were found to be sent from gmail and private email ID to ATM card vendor of the bank.
8) History file was modified after incident.
9) Logs were not present in test server.
10) Suspected IP address and unwanted open port were found in firewall.

Reference snapshots:



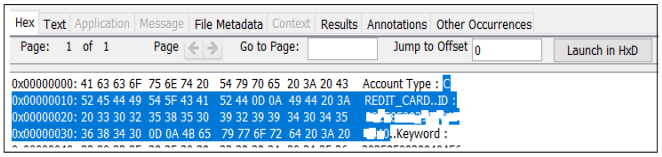


Figure 7: Deleted ATM Script commands and Credit Card Entries

Modus Operandi:

1) Unidentified group/person found vulnerability in Bank's SWIFT Server, Bank's network and they collected all vendor details of the Bank.
2) Sent the phishing email through bank's vendor to bank employee.
3) They infected the IT infrastructure of the target with Malware and identified where a server running SWIFT software and CBS. Also captured all network details including information of devices and their vulnerability.
4) Another requirement which need to be collected by attackers they collected basic IT security level of bank.
5) They downloaded additional malware (droppers) to interact with SWIFT software and CBS which tried to drain the organization's account.

6. Related Work and Proposed Plan

Observations and future proposed plan:

1) Time limit of transaction (Suppose, there have 40K transaction limit and person initiated 2K transaction then transaction will not take more than 30 Seconds to withdraw money. Even though person initiate 40K amount from ATM then also time period should be fixed up to maximum 2 Minutes with high volume of currency).
2) On crossing the limit of transaction time, an alert should be generated to the bank and customer.
3) Monitoring system is must in internal bank system for IT surveillance.
4) Our proposed future plan to elaborate the behavior and structure of malware.

7. Conclusion

In this paper we represented the working of banking ATM and execution of the malware forensic analysis. Examiners face many challenges in live forensic such as timestamp issue, cloud storage, volatile memory analysis, No proper incident response on the crime scene and virtual environment. The proposed work about the onsite crime scene and live forensic of bank being compromised/hacked has been done using EnCase Software and open source tools to detect the malware and its functionality. The normal working of Indian banks and loop holes in bank systems were analysed. Instead of going for multiple forensic/scientific tools, choose specific tools for different environment and create our own custom-action for forensic analysis. Checked existing hash sets adding manual EnScript. The main aim of completed task was to understand workflow of banking system and security analysis on it has been elaborated using well known scientific tools. In addition, there was no appropriate method or way to detect malware in deleted and Unallocated space. Reverse engineering and crime scene reconstruction required improvement in such cases.

8. Acknowledgement and Future Research

This work was done under the Deputy Director Mr. R N Kokare, Regional Forensic Science laboratory, Pune Government of Maharashtra. In future, we will represent the working of malware and its behaviour which was detected in crime scene (Bank).

References

[1] "The biggest cyberheists, in Bangladesh" https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180244/Lazarus_Under_The_Hood.pdf
[2] Threat analysis SWIFT system and the SWIFT Customer Security Program. https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf
[3] Summary of attack in which attackers deploy malware to obtain operator access, SWIFT ISAC Security bulletin 10060, 12 June 2018
[4] https://www.elprocus.com/automatic-teller-machine-types-working-advantages/
[5] Standard operating procedures for collection of Digital evidence‖, v2, June, 2014: Digital Forensic CoE, Enterprise Security and Risk Management, TCS, Hyderabad.
[6] Indian Information Technology Act, 2000 http://www.dot.gov.in/sites/default/files/itbill2000_0
[7] Design and Implementation of Anti-theft ATM Machine using Embedded Systems, Raj M, Anitha Julian, 978-1-4799-7075-9/15/$31.00 ©2015 IEEE
[8] A Similarity based Technique for Detecting Malicious Executable files for Computer Forensics, Jun-Hyung Park1, Minsoo Kim2, Bong-Nam Noh3.