International Journal of Computer Science, Communication & Information Technology (CSCIT)
Vol.7 pp. 17-21

Hack the Bank and Best Practices for Secure Bank

Trust Tshepo Mapoka [#1], Keneilwe Zuva[*2], Tranos Zuva[#3]

[#]*Cyber Security Centre of Excellence (CSCE)*
Cyber Intelligence Agency
Gaborone, Botswana
[1]ttmapoka@ciabotswana.com

[*]*Department of Computer Science*
University of Botswana
Gaborone, Botswana
[2]zuvak@ub.ac.bw

[#]*Department of ICT*
Vaal University of Technology
Vanderbijlpark, South Africa
[3]tranosz@vut.ac.za

***Abstract*— Financial institutions are tremendous targets of opportunity for electronic thievery. Intermingled threats, improvements to man-in-the-middle or browser exploits, and advances in malware diversity has resulted in to easy hacks in to the banks by even less-skilled cybercriminals. The hacks usually targets target something that is of utmost value such as customer credentials and money in the Bank. Historically, banks have purchased various systems to manage threat risks, however their existing perimeter defense controls don't necessarily integrate well. Banks typically have had various fraud prevention controls with various tools for each type of exploit. Further, as these exploits continue to blossom, regulators have struggled to figure out best practice recommendations. Payment Card Initiatives and other banking regulations are a great start, but they haven't kept up with the online threat landscape. This paper addresses many ways of hacking the bank and recommend best practices to securing online banking transactions.**

Keywords—financial crime, secure banking, fraud, cybersecurity

I. INTRODUCTION

The emergence of Internet over a decades has indorsed people to adopt an all connected attitude in expediting their daily tasks [1]. Above all, the usage of internet has attracted the banking sector at large by introducing internet or online banking. The emergence of internet banking has enabled financial institutions to offer their customers relatively convenient and flexible banking, also referred to e-banking. Basically, e-banking refers to bank customers utilising the internet to perform financial services such as online transactions [2]. Online transactions include but not limited to fund transfers, account management and bill payments. Furthermore, e-banking enables ubiquitous online access to the bank accounts without travelling to the bank branch [3]. Internet banking has also benefited both banks and customers because banks have diminished their operational costs by decreasing physical facilities involving human resources, paperwork, and supporting staff. Many countries have integrated the use of the internet into their traditional banking system.

Despite the benefits that the banks are offering through e-banking with faster access to various financial activities [4, 5], there are security concerns that accompany the e-banking systems. [6]. Threat actors widely known as hackers have emerged diversity of intangible techniques for hacking the bank. Though numerous rewards of utilizing e-banking, security issues discourage customers from accepting online usage. This has brought fear to many customers having discovered that online banking usage expose their financial information assets (private credentials, money) at risk [7, 8].

Meanwhile, most banks are widely accepting online usage through the internet, a cumulative number of hackers commit their time to conduct fraudulent activities by using online banking system. It has also emerged in recent research studies that banks can be hacked in so many ways that will be described fully in this paper [9, 10].

This paper is arranged as follows; Section II describes various ways of hacking the bank, Section III describes examples of recent hacking incidents along with the most common hacking types in banks, Section IV describes the true facts about SWIFT and how it correlates with banks from the security perspective. Section V gives the current recommendations that banks can adopt to enhance security. Finally the future strategic best practices for securing the bank are discussed in Section VI.

II. HACKING THE BANK

There are various methods that can be exploited by the threat actor to hack the bank:

- Downloading malicious software in to the enterprise network.
- Social engineering tips to get in to the infrastructure (servers, systems).
- Use of affected peripheral devices such as external USBs.
- Use of Weak cipher suites (SSL/TLS) from web applications.
- Malicious account takeover (Command and Control) which has now increased by greater than 150%.

ISSN 1737-930X

- Use of weak perimeter controls to defend (Anti-virus.
- Connect to any network is undesirably.
- Total access and control to untrusted private bank sites.

Above ALL, the common weak point that the threat actors/hackers take advantage of is the internal staff or people who have interacted or have prior knowledge about the banking system.

A. Most Common Hacking Types

The most common hacking types in financial institutions include:

- Online and Mobile fraud,
- Phishing scams (misleading emails, pop ups or messages) and malware.
- Distributed Denial of Service (DDoS),
- Money Mule scams (triggers the use your own account to perform illegal money transactions),
- Social networking risks and identity theft..

III. SIMILAR HACKING ATTEMPTS RECENTLY

A series of recent bank heists or attempted heist follows malware enabled SWIFT transfers where bank officials received through phishing attempt a malware disguised as the PDF reader.

This is what happens: Attackers conduct months' worth of reconnaissance (study the banks internal processes and controls) before attempting to submit fraudulent SWIFT messages and route bank funds to attacker controlled offshore accounts. In simple context, the hackers use the knowledge and access gained during reconnaissance to begin submitting fraudulent money orders to webs of offshore companies hence enabling them to siphon off millions of dollars. The hackers usually use banks publicly available information and tools to penetrate then commit the theft. The perpetrators gain access to the credentials of those authorized to create and approve messages. The perpetrators then have the capability to send fake messages via Bank computers/systems that interface with the SWIFT system, which enables financial institutions to exchange information on transaction details.

Recently, dozens of Banks mostly in Russia and Ukraine surfaced with unprecedented massive hit of fraudulent enabled SWIFT transfers which led to Hundreds of millions of Dollars being stolen and some salvaged.

A. Banco De Chile loses $10Million in SWIFT Related Attack.

The bank in May 24 2018 surfaced a malware attack then lost about $10 million due to fraudulent SWIFT wire transfers. The compromise occurred while the bank was dealing hundreds of workstations and servers that suddenly ceased working. The malware targeted the bank work stations, affecting cashiers and hampering branch services and phone banking. Some funds were successfully transferred to Hong Kong [11].

B. Hackers siphon $100 Million from Bangladesh Central Bank's reserve Account in New York

The incident follows a malware SWIFT related transfer heist at the BCB reserve Bank in New York. This took place in February 2016, when instructions to fraudulently withdraw US$ 1 billion from the account of Bangladesh Bank, the central bank of Bangladesh, at the Federal Reserve Bank of New York were issued via the SWIFT network. Five transactions issued by security hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines (about $18 million recovered).The Federal Reserve Bank of New York blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank. It was identified later that Dridex malware was used for the attack. Basically, the attackers were able to move laterally within the banks' networks with direction from the attackers' command-and-control servers, compromise administrators' credentials and use those credentials to execute their attacks [12].

C. Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift

It was revealed that revealed that cyber criminals exploited the SWIFT international banking system to steal US$ 10 million from a Ukrainian bank. The theft was conducted in a way similar to the one the Bangladesh central bank experienced earlier this year – when cyber criminals stole about US$ 81 million from the bank [13].

D. Tien Phong Bank in Vietnam in May

In May 2016, such similar fake transfer requests were also used in an attempt to steal more than US$ 1.1 million from the Tien Phong Bank in Vietnam [14].

E. India's Cosmos bank raided for $13m by hackers

Cosmos Bank in India says that hackers made off with $13.4m in stolen funds through Money mule and SWIFT related attacks. Multiple reports out of the country say that a group of attackers used cloned cards to withdraw cash from ATMs at a set time and perform a fraudulent SWIFT money transfer. Together, the efforts resulted in about $13.4m being stolen from the bank and its account holders. The attack was believed to have taken place in two phases. The first attacker was an international effort with money mules in 28 different countries, all extracting cash from their local ATMs. According to the Hindustan Times, 15,000 transactions were carried out over the seven-hour period. The second phase when a SWIFT transaction saw Cosmos move $1.93m to an account at a bank in Hong Kong [15].

IV. TRUE FACTS ABOUT SWIFT

SWIFT is a Brussel based cooperative that interconnect about 11 000 banks worldwide, thus making it attractive and widespread target to the threat actor. However, attackers haven't yet exploited any specific vulnerabilities within the SWIFT system but rather sort to exploit the weak controls at the Enterprise networks for the Banks [16, 17]. The threat actor then compromise key accounts for bank officials in order to create fraudulent transfers. Since the breath taking

ISSN 1737-930X

attacks, Banks around the world have seen attempts to undermine the SWIFT infrastructures but to its credit, SWIFT has tripled its security team by launching a 24/7 Security Operation Centre (SOC) that performs real time monitoring of emanating cyber threats and vulnerabilities. In addition, the SWIFT raise continuous awareness to users and improve security by sharing attack related information. Therefore it is the responsibility of the Banks to up their game with proactive defensive controls to triple the impact of the existing security [18-20].

V. RECOMMENDATIONS FOR NOW

To help protect your Bank from security breaches, you should adopt best practice internal controls [21] and guidelines like the following:

A. Enhance Identity verification during logon

Bank MUST at all times adopt multi factor authentication such that during system logon attempt, the system interact with the actual entity attempting to login. E.g. utilize combination of factors such as Credentials plus OTP sent through text to the mobile phone. Geolocation, pattern based or face recognition factors can be incorporated if desired.

B. Implement Dual Custody during Transactions

Adopt dual authorization and/or transaction-based authentication procedures during financial transfers. Identify verification should adopt real time interaction with the actual entity performing the transaction (Multi factor authentication must apply during transfers).

C. Creating and Protecting Credentials password.

Adopt best practice when creating passwords such as use of combination of alphanumeric characters (./?!#@%*&), One upper case letter, 2 numbers. Bank users SHOULD never share login credentials with anyone and SHOULD never write it down. Use a secure password manager if you need help keeping track of many passwords.

D. Protect your Machines

Place limits and controls on who has access to your computer systems. Users should avoid or cancel the remember passwords prompt on online banking login sites. Make sure the bank's computers are running the latest operating system and versions of software, web browser, and anti-virus protection. Automatic update with security fixes is key. Users should not do your online banking from a computer that has unknown perimeter control status.

E. Routine Risk and Vulnerability Assessment

Since no risk and vulnerability assessment has been carried out before:

It is important for the Bank to know its security posture from the risk perspective. Threat actors take advantage of exploitable vulnerabilities that exist within enterprise (corporate) network points (endpoints, systems, servers) to penetrate deep in to something that is value (i.e. systems that does money transfers, user credentials for online, user privilege escalation procedures). Therefore, recommend the bank to perform routine vulnerability assessment for entire system in combination with Penetration test in the perspective of the hacker. The results will determine the vulnerabilities that can exploited and tested against the existing perimeter controls then report on remediation control measures (necessary patching) that should be in place to maintain protection.

From the risk assessment perspective, routine risk assessment screening must be performed in this context so that any employee contractor, or third party user termination or change of employment or responsibilities cannot result in to deliberate breach. Usually the ex-employees/contractors/third party users understand the banking system and have the credentials at termination. Therefore termination procedures between the Human resource and IT resource must be in place to ensure immediate disabled access of the terminated within the AD or any other related security access to the enterprise and disable access to the facility to avoid future disgruntled breaches. Risk assessment must be performed Prior to employment, during employment and after employment (termination) to maintain up to date records.

1) Tools for Vulnerability Risk Management: Majority of the Banks are now integrating real time vulnerability and risk management tools in to their Enterprises to ensure real time visibility and analytics of risk threats attempting to impact business systems, endpoints, servers etc. In this case you can proactively identify, prioritize, and remediate vulnerabilities before being breached.

Desired Tools in the market: InsightVM, Qualys Enterprise Suite

F. Routine Cyber fraud awareness

Employees need routine awareness on current Cyber heist to be cautious and suspicious, and never take e-mail at face value – especially if it seems urgent or contains threats. These may be phishing attempts designed to trick people into opening a malicious link or attachment. They should know to always check any suspicious or unexpected communications by calling, e-mailing, or going to a website directly instead of clicking any links.

G. Compliance to Security Standards

Banks should strictly to adhere to international best practice standards (e.g. ISO 17799 and 27001, PCI-DSS) to avoid unprecedented breaches. Proper information security policies and procedures should adopt international best practice. Failure to meet regulatory guidelines can result in severe penalties for financial institutions [22,23].

VI. FUTURE STRATEGIC SECURITY INITIATIVES

Due to persistent cyber heists affecting Banks recently, I suggest the following:

- Proactive approach to Cyber security [24-26]: Establish Unified Security Operations and Analytics platform known as the Cyber Security Operation Centre (CSOC/CERT/CSIRT/CIRT) similar to the SWIFT SOC. The CSOC [27-29] shall integrate with the existing perimeter controls acting as perimeter wall that provides overall visibility and proactive real time monitoring over evolving (insider and outsider) threats and vulnerability exploits targeting the Bank enterprise network systems. Early detection and prevention is better than cure. The centralised platform consists of incident response management team that promote information sharing on current surfaced threats targeting the Bank. If you cannot afford the

ISSN 1737-930X

establishment then outsource through reputable Managed Security Service Provider (MSSP) so that you are monitored 24-7-365 days.

- Enhance strong information sharing capability of emanating security incidents with SWIFT.
- Eliminate single sign on factor and expand to multi-factor support to authenticate SWIFT messages
- Enhance security and audit risk baselines for participating banks,
- Increase integrity support for anomaly detection and stop-payment controls,
- Engage third-party consultants to assist with security assessments and implementation
- Adopt analytics technology that performs Darkweb monitoring [30] for threats that occur in the dark space such as Blockchain (Bitcoins).
- Carry out risk assessment by updating the employee credentials database such that terminated officials have disabled access to the VPN, ADs and disabled physical access to sensitive facility areas.
- Carry out vulnerability assessment to proactively identify, prioritize, and remediate vulnerabilities before being breached.

REFERENCES

[1] Razak LT(2016). The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM" Mohammed A. Al-Sharaf,"Ruzaini A. Arsha," Emad Abu-Shanab and "Nabil Elayah" Faculty of Computer Systems and Software Engineering, UMP. Journal of Engineering and Applied Sciences, 100, 545-552.

[2] Jolly V(2016). The Influence of Internet Banking on the Efficiency and Cost Savings for Banks' Customers. International Journal of Social Sciences and Management, 3, 163-170.

[3] Safeena R(2010). Customer perspectives on E-business value: case study on Internet banking. Journal of Internet Banking and Commerce. 15, 1-17.

[4] Sharma S(2016). A detail comparative study on e-banking VS traditional banking. International Journal of Advanced Research, 2, 302-307.

[5] Konoth RK, van der Veen V, Bos H(2016). How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security.

[6] Vaciago G, Ramalho DS(2016). Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence & Elec. Signature L. Rev., 13, 88.

[7] Balk R, Yap BK, Loh C, Wong HD(2009). To trust or not to trust: the consumer's dilemma with e-banking. Journal of Internet Business, 6,1-27.

[8] Leukfeldt ER, Kleemans ER, Stol WP(2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. British Journal of Criminology, 9.

[9] Chiu CL, Chiu JL, Mansumitrchai S(2016). Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation. International Journal of Financial Services Management, 8, 240-271.

[10] Arachchilage NAG, Love S, Beznosov K(2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, 185-197.

[11] Bank info Security News. J Kirk (2018, Jun. 13). Banco de Chile Loses $10 Million in SWIFT-Related Attack [Online]: https://www.bankinfosecurity.com/banco-de-chile-loses-10-million-in-swift-related-attack-a-11075.

[12] New York Post. K Dugan. (2016. Mar 7). Bangladesh bank says hackers stole $100M from its New York Fed account [Online]: https://nypost.com/2016/03/07/bangladesh-bank-says-hackers-stole-100m-from-its-new-york-fed-account/.

[13] Occrp News. I Spaic. (2016. Jun 28). Ukraine: US$ 10 Million Stolen From Unnamed Bank via Swift [Online]: https://www.occrp.org/en/27-ccwatch/cc-watch-briefs/5419-ukraine-us-10-million-stolen-from-unnamed-bank-via-swift.

[14] The Wall Street Journal. T Khanh Vu, K Burne (2016. May 16). Vietnam's Tien Phong Bank Targeted in Bangladesh-Like Cyberattack [Online]: https://www.wsj.com/articles/vietnamese-bank-says-it-was-target-of-attempted-cyber-heist-1463405095.

[15] Wn.com news. ZDnet (2018. Aug 27). How_hackers_managed_to_steal_135_million_in_Cosmos_bank_heis [Online]: https://article.wn.com/view/2018/08/27/How_hackers_managed_to_steal_135_million_in_Cosmos_bank_heis/

[16] Kumar Parekh, Society for Worldwide Inter bank Financial Telecommunication, 2006.

[17] SWIFT routing protocol, 2007, [online] Available: http://www.swift.com.

[18] Roberto Andrade, Jenny Torres, Pamela Flores, "Management of information security indicators under a cognitive security model", Computing and Communication Workshop and Conference (CCWC) 2018 IEEE 8th Annual, pp. 478-483, 2018.

[19] Shakeel Durrani, Imran Jattala, Junaid Farooqi, Naila Shakeel, Mohsin Murad, "Design and development of wireless RTU and cybersecurity framework for SCADA system", Information & Communication Technologies (ICICT) 2013 5th International Conference on, pp. 1-6, 2013.

[20] Jan M. Ahrend, Marina Jirotka, Kevin Jones, "On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge", Cyber Situational Awareness Data Analytics And Assessment (CyberSA) 2016 International Conference On, pp. 1-10, 2016. SOC

[21] Siddharth Mahajan, Mitesh Parekh, Hardik Patel, Sharvari Patil, "BRB dashboard: A web-based statistical dashboard", Innovations in Information Embedded and Communication Systems (ICIIECS) 2017 International Conference on, pp. 1-6, 2017.

[22] Rigon Alencar, E. Merkle, C. Westphall, Santos, D. Ricardo dos, C. Becker Westphall, "A cyclical evaluation model of information security maturity", Information Management & Computer Security, vol. 22, no. 3, pp. 265-278, 2014.

[23] 2. Y. Cherdantseva, J. Hilton, "A reference model of information assurance & security", Availability reliability and security (ares) 2013 eighth international conference on, pp. 546-555, 2013, Septembe

[24] Marina Danchovsky Ibrishimova, Advances on P2P, Parallel, Grid, Clou Andrea Dufkova, "National/governmental CERTs ENISA's recommendations on baseline capabilities" in , Enisa Publications.

[25] 2. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, "Recommendations of the National Institute of Standards and Technology", NIST.

[26] 3. Carnegie Mellon, "Creating and Managing Computer Security Incident Handling Teams", CERT Training and Education. d and Internet Computing, vol. 24, pp. 469, 2019.

[27] Zahra Zohrevand, Uwe Glasser, Hamed Yaghoubi Shahir, Mohammad A. Tayebi, Robert Costanzo, "Hidden Markov based anomaly detection for water supply systems", Big Data (Big Data) 2016 IEEE International Conference on, pp. 1551-1560, 2016.

[28] Boyeon Song, Sang-Soo Choi, Jangwon Choi, Jungsuk Song, Information Security, vol. 10599, pp. 437, 2017.

[29] Boyeon Song, Jangwon Choi, Sang-Soo Choi, Jungsuk Song, "Visualization of security event logs across multiple networks and its application to a CSOC", Cluster Computing, 2017.

[30] Eric Nunes, Paulo Shakarian, Gerardo I. Simari, "At-risk system identification via analysis of discussions on the darkweb", APWG Symposium on Electronic Crime Research (eCrime) 2018, pp. 1-12, 2018.

ISSN 1737-930X

Dr. Trust T Mapoka received BEng and MEng degrees in Telecommunications and Internet Engineering from University of Bradford, United Kingdom, in 2010 and 2011 respectively. He obtained PhD. Degree in Cybersecurity from university of Bradford, UK in 2016. He hold professional certifications such as Certified Ethical Hacker (CEH), Certified Network Defense Architect (CNDA), Certified Information Security Management Principles (CISMP). He is member of IEEE and IET. He is currently the Senior Cyber Security Expert and provide consultancy on various expertise of Cybersecurity that include Security Operations Analytics, Fraud Management, Ethical Hacking and Vulnerability Management, User Entity Behavioral Analytics (UEBA), Incident Dectection and Response, Network Forensics and Auditing, Identity Spoofing and Training and Awareness. Research interest include IoT Security analytics, Light Cryptography, Wearable devices security, Security Information and Event Management (SIEM) technologies for IoT security, Data Mining, Business Intelligence.

Mrs. Keneilwe Zuva is a Senior Lecturer in the Department of Computer Science at University of Botswana. She holds a Master of Engineering (Information Systems and Networks) from the University of Essex in United Kingdom. Her research interests are in Recommender Systems, Computer Networking and Cyber Security threat detection and Analytics, Network Forensics Auditing, Perimeter defenses, multi factor Authentication, Cryptography, IoT security.

Prof. Tranos Zuva is an Associate Prof in the Department of ICT in Vaal University of Technology, South Africa. He has published extensively in computer science field. His research areas include recommender systems, networking, Data mining, Business Intelligence and image processing. He is a IEEE member.

ISSN 1737-930X