JACKPOTTING AND THE CANADIAN BANKING ENVIRONMENT

Date: September 19, 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

EXECUTIVE SUMMARY

Insightful intelligence and analysis can be conducted using open-source intelligence data and careful analysis. This article used open sources and conducted a variety of validation checks to ensure an accurate as possible assessment. It can serve as a platform for presenting a national security issue and asking a probative question.

KEY EVENTS

This briefing note addresses the following events which raise concerns about Automated Teller Machines' (ATM's) security vulnerability to cyber-attacks: 1) The FBI's September 2018 warning of an imminent global heist (Gonzalez, 2018); 2) Eleven countries in Europe experiencing a total of 114 cash out attacks, resulting in an over 300 percent increase in attacks since 2016 (Zykov, 2017); 3) A series of cyber-attacks occurring against financial institutions resulting in $45 million USD being withdrawn from ATMs in New York (Seifert, 2013), and a similar cyber-attack resulting in $2.4 million USD being stolen from a Blacksburg, VA bank in two attacks during May 2016 and January 2017 (Crossman, 2018); 4) the most recent attack August 10 - 13 (2018) at Cosmos Bank (India) which netted approximately $13.5 million USD from 14,800 transactions across twenty-eight countries (Brusnashan, 2018). Within a Canadian context, in 2014, two fourteen year-old teenagers were able to break into a Bank of Montreal ATM. Caleb Turon and Matthew Hewlett used an online manual, guessed the administrator password, and changed the surcharge to one cent. They also changed the display screen to read "Go away. This ATM has been hacked" (Pauli, 2014).

NATURE OF DISCUSSION

This briefing note explores the following issues: What an ATM is, what the financial costs and lost opportunity impacts on the banking sector are, what a Jackpotting attack is, how financial institutions are planning to harden ATMs against Jackpotting if possible, and what the Canadian national security connection is.

BACKGROUND

Cybercrime reporting continues to be refined to provide accurate assessments and public information. A survey of the newsfeeds would suggest cybercrime is an everyday occurrence; however, as noted in Crossman's (2018) article, "we are not yet sure...whether the FBI warning is based on verified facts," which is a reminder that agencies need to be cautious about reporting cybercrime (para. 12).

The data needed to validate a cybercrime is complex, large, multijurisdictional, and requires due diligence in collection and interpretation. For example, Free ATM Processing (2016) reported, citing ATMIA's 2016 ATM fraud study, that ATM crime fell from fifty-one percent in 2015 to forty-two percent in 2016. When this claim by Free ATM Processing was fact checked, it was revealed that the primary source's (ATMIA, 2016) wording was "percentage of respondents reporting a general increase in ATM crime fell from fifty-one percent in 2015 to forty-two percent this year" (ATMIA, 2016; Free ATM Processing, 2017). In other words, forty-one percent of survey participants are still reporting increased ATM crimes being experienced. Cybercrime reporting and the impact of cybercrime on victims and society is problematic due to changing intelligence about the crime, continual revisions on threat assessment findings, and continual debate about what criminal activities and network vulnerabilities to include when conducting threat assessments.

Automated Telling Machine (ATM) is an automated banking machine which allows customers to complete basic transactions without the help of a bank representative. The ATM is essentially a computer consisting of a keyboard, card readers, speakers, display screen, printer, and cash depositor. The ATM's computer is connected to a host computer, which then connects to the bank's computer. These connections are provided by the Internet Service Provider (ISP). The ATM, the host computer and the bank computer use a centralized database system to manage the transaction data. These computer networks and centralized database have known vulnerabilities which are exploited by the criminal

(Trendmicro, 2018; Agarwal, 2018). These vulnerabilities are discussed in the defending against jackpotting/ cashing-out attacks section below.

ATM attacks consist of physical attacks and network-based malware attacks. These attacks may exploit the vulnerabilities of the client's ATM card, which has the magnetic strip and a chip containing the customer's data. It is also possible that these attacks exploit the vulnerabilities of the underlying computer technology using logic attacks. This report focuses on the logic attacks. An example of this is the Ploutus-D malware which has been used by criminals to infect Opteva 500 and 700 series ATM produced by Diebold (Paganini, 2018). Ploutus was discovered in Mexico in 2013 and it allows criminals to access the ATM with an external keyboard or by sending it SMS messages. FireEye Labs has found a new version of Ploutus which exploits KAL's Kalignite multivendor ATM deployed around the world in eighty countries. Its primary purpose is to empty the ATM without requiring an ATM card (Regalado, 2017).

Defending against jackpotting/cashing out attacks includes countermeasures such as the following: physically locking down access to the ATM's USB ports, turning off or deleting unnecessary software such as online video games loaded with Windows environment, restricting third-party vendor access, implementing inventory control and destruction of spare ATM parts, and supporting user education (PCI Security Standards Consulting, 2013). One countermeasure developed by MasterCard Inc. is called Safety Net, and it utilizes machine-learning technology to monitor transactions. It has been instrumental in detecting and controlling three separate cyber-attacks, which included targeting ATMs. In these three examples, the cybercriminals managed to steal less than $100,000 each. In a similar attack in 2013, before Safety Net was built, criminals penetrated internal systems at a bank in the United Arab Emirates. They raised cash-withdrawal limits on twelve prepaid MasterCard debit card accounts, according to a federal complaint. They made fake cards using the stolen account numbers, then at a pre-planned time, fanned out across countries to withdraw cash from ATMs (Nash, 2016).

Why jackpotting is a potential national security issue for Canada. Attacking ATMs and banking systems is not new. For example, an unsealed indictment from the Manhattan Federal Court revealed that, beginning in 2011, Iran-based hackers began hacking the New York Stock Exchange, Nasdaq, Bank of America, JPMorgan Chase, AT&T, and others, on behalf of the Islamic Revolutionary Guard Corps. One of them gained unauthorized remote access to a computer controlling the Bowman Avenue Dam in Rye, N.Y., for about three

weeks in 2013. On some days, the hacking prevented hundreds of thousands of banking customers from accessing their accounts, according to the indictment, costing the banks tens of millions in remediation efforts (American Banker, 2016).

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Explicitly related to Jackpotting, can Plotous malware and its variants be used in Canada? In anticipation of cybercriminals adapting to major banks and credit unions, what efforts need to be made to protect Canada's small and medium enterprises that have ATMs?

Questions relating specifically to the Islamic Revolutionary Guard, and to the associated SOBH Cyber Jihad claiming responsibility for Bowman Avenue Dam incident. Does this dam share similar operating systems with Canadian dams? Is there evidence of them operating in Canada or funding Canadian radicalization efforts? More importantly, why was that particular dam targeted? Alternatively, did the SOBH, as speculated by the mayor of the city where the dam is located, attack the wrong dam? (Berger, 2016). Either way, the terrorist did succeed in being able to conduct a cyber operation against the dam. Are similar dam software controls operating in Canada?

Questions relating specifically to the Bowman Avenue Dam cyberattack being overstated by media. According to a security blog post by Robert M Lee of SANS Industrial Control Systems on December 21, 2015, details reported suggested this was not an intrusion, but a Cyber Kill-chain Reconnaissance in Stage 1 (Lee, 2015). What efforts or lessons learned can be formulated to help law enforcement, computer emergency response teams, and the media formulate a strategy to use correct language to report a cybersecurity incident accurately? Moreover, how is this issue being addressed in Canada?

References

Agarwal, T. (2018). How ATMs work? *EL-PRO-CUS (nd).* Retrieved from https://www.elprocus.com/automatic-teller-machine-types-workingadvantages/

American Banker. (2016). U.S. Charges Iranian Hackers in Wall Street Cyber-Attacks. *American Banker (Mar. 24, 2016).* Retrieved from www.americanbanker.com/news/us-charges-iranian-hackers-in-wallstreet-cyber-attacks

ATMIA. (2016). ATM industry association releases results for 2016 global fraud and security survey. *ATMIA (Dec. 21, 2016).* Retrieved from www.atmia.com/news/atm-%20industry-association-releases-resultsfor-2016-%20global-fraud-and-security-survey/4394/

Berger, J. (2016). A dam, small and unsung, is caught up in an Iranian hacking case. *New York Times (Mar. 25, 2016).* Retrieved from www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-incomputer-hacking-case.html

Brusnashan, P. (2018). $10 million stolen in global bank heist. *Verdict Cards International (Aug. 16, 2018).* Retrieved from https://www.verdict.co.uk/cards-international/news/bank-heist-globalatm/

Crossman, P. (2018). How worried should banks be about the FBI's ATM attack warning? *American Banker, 183(158), np.*

Free ATM Processing. (2017). As ATM Crime falls, challenges remain. *Free ATM Processing (Feb. 17, 2017)*. Retrieved from www.freeatmprocessing.com/atm-fraud/as-atm-crime-falls-challengesremain/

Gonazalez, G. (2018). The FBI is warning banks about an imminent global heist. *Inc, (Aug. 14, 2018)* . Retrieved from www.inc.com/guadalupegonzalez/fbi-warns-global-bank-heist-atm-cash-out.html

Lee, R. (2015). Takeaways from reports on Iranian activity against the power grid and a dam. *Sans Industrial Control Systems Security Blog (Dec. 21,*

2015). Retrieved from https://ics.sans.org/blog/2015/12/21/takeaways-from-reports-oniranian-activity-against-the-power-grid-and-a-dam

Nash, K. (2016). MasterCards' machine-learning network thwarts ATM attacks. *CIO Journal (Feb. 23rd, 2016).* Retrieved from www.blogs.wsj.com/cio/2016/02/23/mastercards-machine-learningnetwork-thwarts-atm-attacks/

Paganini, P. (2018) Crooks target ATMs with Ploutus-D malware, these are the first confirmed cases of Jackpotting in US. *Security Affairs (Jan. 30, 2018).* Retrieved from www.securityaffairs.co/wordpress/68412/cyber-crime/jackpottingus.html

Pauli, D. (2014). Kids hack Canadian ATM during lunch hour. *The Register (Jun. 12, 2014).* Retrieved from www.theregister.co.uk/2014/06/12/kids_hack_canuck_bank_atm_during_lunch_break/

PCI Security Standards Council. (2013). Information Supplement: ATM Security Guidelines. PCI Security Standards Council, LLC: Wakefield, MA.

Regalado, D. (2017). New variant of Ploutus ATM malware observed in the wild in Latin America. *FireEye (Jan. 11, 2017).* Retrieved from www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html

Seifert, D. (2013) 'Criminal flash mob' accused of stealing $45 million in hours with coordinated ATM attacks. *The Verge, (May 9, 2013).* Retrieved from https://www.theverge.com/2013/5/9/4316626/criminalflash-mob-accused-stealing-45-million-hours-atm-attack

Trendmicro. (2018). Cashing in on ATM malware: A comprehensive look at various attack types. Trendmicro: Irving, TX.

Zykov, K. (2017). ATM jackpotting for dummies;Yours for just £3,788. FineExtras, (Oct. 18, 2017). Retrieved from www.finextra.com/newsarticle/31210/atm-jackpotting-for-dummiesyours-for-just-3788

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: https://jicw.org/