Jackpotting and the Canadian Banking Environment
Date: Sept 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.

KEY EVENTS

This note addresses the following events which raise concerns about Automated Teller Machines' (ATMs) security vulnerability to cyberattacks. 1) FBI's September 2018 warning of a imminent global heist. 2) 11 countries in Europe experiencing a total of 114 cash out attacks (more than 300% increase in attacks) since 2016, 3) A series of cyberattacks against financial institutions resulting in $45 million (US) being withdrawn from ATMs in New York and a similar cyberattack resulting in $2.4 million (US) being stolen from a Blacksburg, VA bank in two attacks (May 2016 & January 2017), and 4) the most recent attack August 10 - 13 (2018) at Cosmos Bank (India) which netted $13.5 million (approx.) from 14,800 transactions across 28 countries. Within a Canadian context, in 2014, two 14 year old teenagers (Caleb Turon and Matthew Hewlett) were able to break into a Bank of Montreal ATM using a online manual, guessing the administrator password, and changing the surcharge to one cent and the display screen to read "Go away. This ATM has been hacked."

NATURE OF DISCUSSION

This briefing note will explore the following issues: What is an ATM? What are the financial costs and lost opportunity impact on the banking sector? What is a Jackpotting attack? How are, or can, financial institutions target harden ATMs against Jackpotting? What is the Canadian national security connection?

BACKGROUND

A word of caution regarding cybercrime reporting. Cybercrime reporting continues to be refined to provide an accurate assessment and public information. A survey of the newsfeeds would suggest cybercrime is an everyday occurrence, and this may be true. However, as noted in Crossman's article "we are not yet sure...whether the FBI warning is based on verified facts" is a good reminder that agencies need to be cautious about reporting cybercrime. The data needed to validate a cybercrime is complex, large, and multi jurisdictional, and requires due diligence in collecting and interpreting. For example, Free ATM Processing (2016) reported, citing ATMIA's 2016 ATM fraud study, ATM crime fell from 51% to 42%. Fact checking Free ATM Processing claim, revealed the primary source (ATMIA, 2016), wording is "percentage of respondents reporting a general increase in ATM crime fell from 51% in 2015 to 42% this year". In other words, 41% 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 revision of threat assessment findings, and continued debate about what criminal activity and network vulnerability to include in when conducting threat assessments.

Automated Telling Machine (ATM) is a automated banking machine which allow 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 computer, these connects are provided by the Internet Service Provider (ISP). The ATM, host computer and 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. These vulnerabilities are discussed in the defending 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 chip containing the customer's data, or, exploit the vulnerability of the underlying computer technology using logic attacks. This report focuses on logic attacks.

One such example is the Ploutus-D malware which has been used by criminals to infect Opteva 500 and 700 series AMT produced by Diebold. Ploutus was discovered in 2013 in Mexico and allows criminals to access the ATM with an external keyboard or by sending it SMS messages. FireEye Labs have found a new version of Ploutus which exploits KALS Kalignite multivendor ATM deployed around the world in 80 countries. Its main purpose is to empty out the ATM without requiring an ATM card.

Defending against jackpotting / cashing out attacks includes countermeasures such as physically locking down access to the ATMs USB ports, turning off / 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 support user education. One countermeasure developed MasterCard Inc. utilizes machine-learning technology to monitor transactions. called Safety Net, it has been instrumental in detecting and controlling three separate cyberattacks which included targeting ATMs. In these three examples, the cybercriminal only stole $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 to raise cash-withdrawal limits on 12 pre-paid 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.

Why this is a Canadian national security issue. The final section of the discussion will be the national connection between state-sponsored actors and Canada's national security. Attacking ATMs and banking systems is not new. For example, "in the Manhattan federal Court an unsealed indictment revealed that beginning in 2011 Iran-based hackers on behalf of the Islamic Revolutionary Guard Groups began hacking the New York Stock Exchange, Nasdaq, Bank of America, JPMorgan Chase, and AT&T, among others, according to an indictment unsealed Thursday in Manhattan federal court. One of them gained unauthorized remote access to a computer controlling the Bowman Avenue Dam in Rye, N.Y., for about three weeks beginning 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".

KEY POINTS OF DISCUSSION AND WEST COAST PERSPECTIVES

Related specifically 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 who have ATM's?

Related specifically to the Islamic Revolutionary Guard, and 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 that particular dam? Or did the SOBH, as speculated by the Mayor of the city where the dam is, attack the wrong dam? 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?

Related specifically to the Bowman Avenue Dam cyberattack being overstated by media. According to Robert M. Lee of SANS Industrial Control Systems security blog posted Dec 21, 2015 details reported suggest this was not an intrusion, but a Cyber Killchain Reconnaissance in Stage 1. 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 accurately report a cybersecurity incident? How is this issue being addressed in Canada?