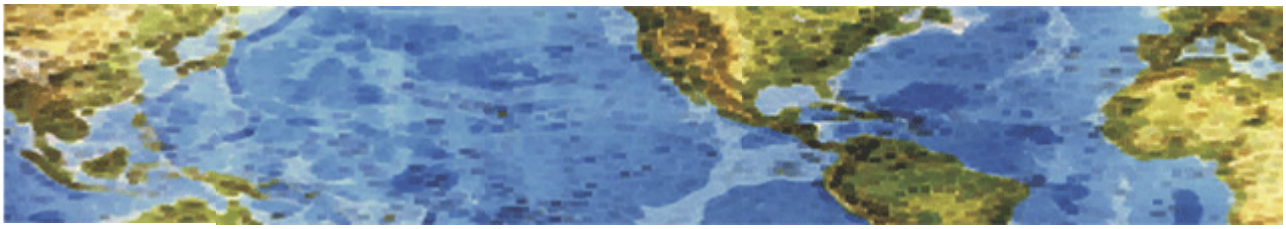
HALL ASSOCIATES



Risk-Based Decision Making Commentary
15 June 2014 Newsletter

Ninth Grade Students Hack into ATM Machine during School Lunch Break

When I was in school, I used played outdoor games like basketball and badminton. When I was in college, I started taking more interest in playing computer games rather going out. But nowadays, children have completely changed their hobbies to programming, hacking and bug bounties in such a ways that in just half an hour of lunch break between classes they hacked an ATM machine.

A pair of ninth grade students, both 14 years old, broke into a Bank of Montreal ATM during their lunch hour between classes by following an old ATM operators manual found online. The duo used the online manual to access the operator mode of the ATM machine in Winnipeg. They didn't use the accessed data to steal any amount from the ATM, rather they simply broke into the ATM machine and printed off information including users' transaction data, surcharge profits and the total cash held in the unit.

HOW THEY HACKED INTO THE ATM MACHINE

They were not expecting the hack to work but when the machine asked for the administrator password and the pair gained access to the data of the machine by their first guess, a six-character long password indicating the ATM had default settings enabled, *The Winnipeg Sun reported Sunday*. The teenagers then immediately reported their hack to bank employees at the BMO Charleswood Centre branch on Grant Avenue, who first assumed the boys had solely acquired the PIN numbers of one of the ATM customers.

> *"I said: 'No, no, no. We hacked your ATM. We got into the operator mode,'" one of the boys said after being asked for the proof of their hack by the bank's head of security. "So we both went back to the ATM and I got into the operator mode again." "Then I started printing off documentations like how much money is currently in the machine, how many withdrawals have happened that day, how much it's made off surcharges. Then I found a way to change the surcharge amount, so I changed the surcharge amount to one cent." To aware ATM users, the duo changed the ATM's welcoming message from "Welcome to the BMO ATM" to "Go away. This ATM has been hacked."*

Neither of the boys are facing any type of criminal charges related to the ATM hacking, instead they're actually being applauded by the bank employees and people online for exposing a serious security risk to the bank and for the honesty of the two. The branch manager even wrote a note to school administrators to excuse both for being late returning from their lunch hour. "*Please excuse these boys for being late during their lunch hour due to assisting BMO with security*," reads the note.

The BMO bank, which has more than 900 branches across Canada with over seven million customers in US, said it was aware of the reported incident and has already taken actions to prevent unauthorized access to its ATM machines, which may have involved changing the default passwords on all of its ATMs.

http://thehackernews.com/2014/06/ninth-grade-students-hack-into-atm.html

HALL ASSOCIATES

Security is a Journey, Not a Destination

Individuals and Organizations Need to Look at Their Security Model Holistically and Gain Continuous Protection and Visibility Along the Entire Journey. You do have a security model, don't you?

Most security tools and policies today focus on prevention only – access control, detection, and blocking at the point of entry – to protect systems. They scan files once at an initial point in time and do periodic scans to determine if they are malicious. But predictably, attackers today fundamentally understand the static nature of these security technologies and **are innovating around their limitations to penetrate network and computer defenses.** The latest improvements in threat detection for systems include executing files in a sandbox for detection and analysis, the use of virtual emulation layers to obfuscate malware from users and operating systems, reputation-based application whitelisting to baseline acceptable applications from malicious ones, and, more recently, attack chain simulation and analysis detection. But if the file isn't caught entering or if it evolves and becomes malicious after entering your computer or network, point-in-time detection technologies are no longer useful in identifying the unfolding follow-on activities of the attacker.

Advanced attacks aren't focused on what we traditionally consider to be the destination – the walls of the network or computer. They're focused on the journey, leveraging an array of attack vectors, taking endless form factors, launching attacks over time, and obfuscating the exfiltration of data. **These new attacks aren't limited to a point in time but are ongoing and require continuous scrutiny**. **In order to detect advanced threats and breach activity more effectively, security methods and policies can't just focus on detection and prevention but must also include the ability to mitigate the impact once an attacker gets in.** Organizations and individuals need to look at their security model holistically and gain continuous protection and visibility along the entire journey – from point of entry, through propagation, and post-infection remediation.

To do this we need a security model that overcomes the limitations of traditional point-in-time detection and response technologies. And it is becoming clear that organizations and even individuals need a security professional to determine how and what they need to do based on their system and type of data to be protected. Ad hoc security has become practically useless in today's cybercrime environment. With a true continuous security model, security professionals can answer key questions like:

- What was the method and point of entry?
- What systems were affected?
- What did the threat do?
- Can I stop the threat and root cause?
- How do we recover from it?
- How do we prevent it from happening again?

In the model we all need today and tomorrow, detection and response are no longer separate disciplines or processes but an extension of the same objective: to stop threats. It's what's required for advanced threat detection and response that's focused on the journey, not just the destination.

http://www.securityweek.com/security-journey-not-destination