



SENTIENT

ATM Jackpotting

Financial institutions lose money & trust

Table of Contents

1. Executive Summary	2
2. Cost of the Threat	2
3. Stakeholder Impact	3
4. How does “ATM Jackpotting” work?	3
5. Sentient to the Rescue	4
6. Summary	5

1 Executive Summary

ATM jackpotting is a cyber-crime where hackers take control of the ATM's computer allowing them to take out cash at will. The malware introduced by the hackers interacts with the ATM's software and hardware, making it relatively easy to dispense cash.

Ostensibly, the bank just loses some money, perhaps a good deal of money across multiple such jackpotting attacks. However, the real cost is much higher. With every such incident, the bank loses trust with its customers. Jackpotting impacts the entire ATM ecosystem, however, it perhaps most impacts the CISOs and risk officers across the financial institutions.

2 Cost of the Threat

Jackpotting criminals have reportedly stolen over a hundred million dollars from ATMs across the globe. The world learned already back in 2009 how susceptible ATMs are to hack. Since then many varieties of malware have emerged, and ATM jackpotting has gained ground. And the fact that most ATMs run on an outdated operating system that have reached "end of support" years ago, paves the path for hackers to continue even more aggressively.





Cybercriminals have now realized that they can not only physically attack ATMs but also access these machines over the network. Once they install malware and get an entry into the network, the potential damage they can inflict is endless. While a fully stocked ATM might yield a \$50,000 haul, compromising an endpoint to a corporate network might lead to tens of millions of dollars of losses. So, the threat is clearly not limited to ATM's.

While a well-stocked ATM may only result in a \$50,000 financial loss, the overall cost of ATM jackpotting runs wider and deeper. The entire ecosystem - everyone from the ATM manufacturer to the end customer suffers.

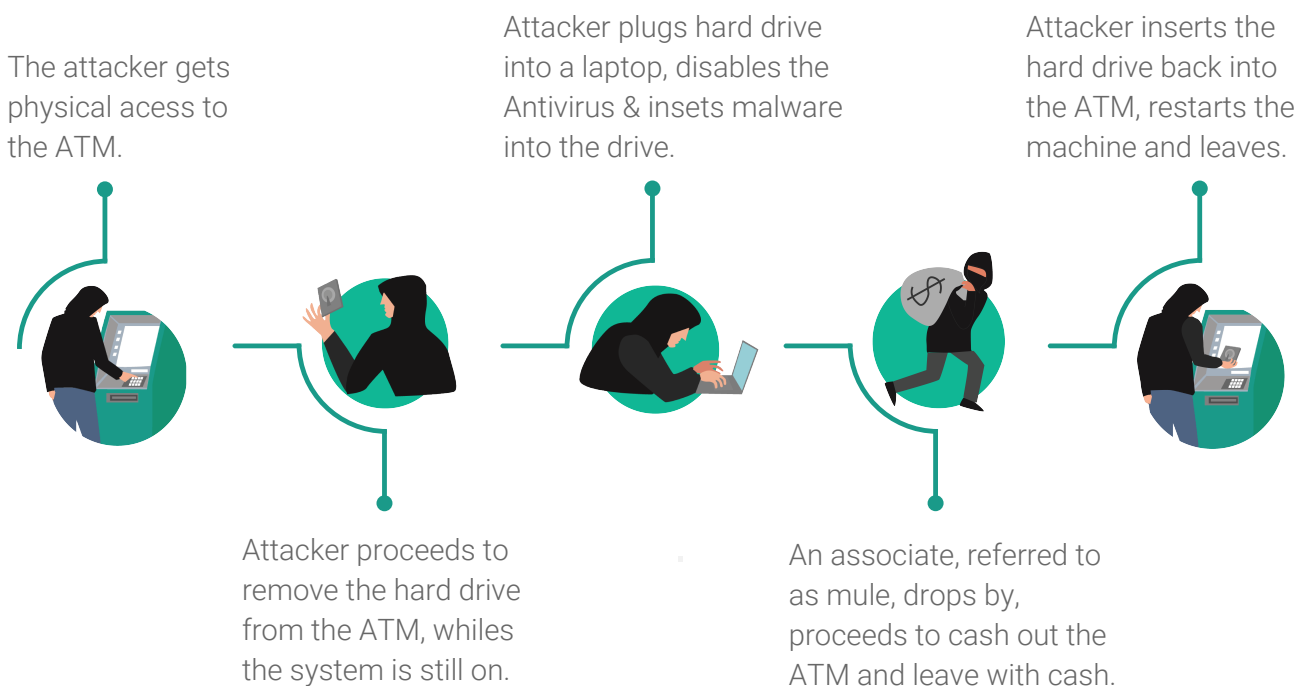
The ATM manufacturers suddenly find themselves in the cross hair of their financial institution customers as well as the law enforcement agencies, who are eager to find how their product could be so easily hacked. This raises issues of credibility, liability and loss of confidence. The problem goes further. Companies that manage ATMs for financial institutions face risks that grocery chains and drug stores might ask them to haul away their ATMs. No business wants its names associated with a crime; these chains would rather have a clean image even if it is a minor inconvenience for their consumer to withdraw cash at the store. The financial institutions, of course, take the worst hit of all. They are the one who lose actual money and are targets for being hit over and over. This has implications for financial losses, insurance but also customer confidence. The final piece in the puzzle is the end consumer. They really are not impacted in any tangible manner; and yet, for most consumers there is the ever-present concern that their data was likely stolen. This does not bode well to build confidence in the financial industry.

Not all is lost though. While no solution can offer an ironclad guarantee to prevent ATM jackpotting, there are ways to mitigate the problem, and continue to strengthen these solutions.

3 Stakeholder Impact

 ATM Manufactures	 Banks	 ATM Maintenance Vendors and Insurance Providers	 Customers
<ul style="list-style-type: none"> - Damaged machines - Risk of malware infection in the ATM network - Tarnished brand equity - Loss of customers 	<ul style="list-style-type: none"> - Tarnished brand equity - Risk of malware infection spreading to the bank infrastructure - Customer inconvenience due to empty ATMs - Loss of customers 	<ul style="list-style-type: none"> - Increased insurance claims against ATM Jackpotting incidences - Loss of customers 	<ul style="list-style-type: none"> - Inconvenience due to lack of cash - Fear that their data might get stolen

4 How does “ATM Jackpotting” work?



5 Sentient to the Rescue

Accelerite's Sentient is an extensible security framework that mitigates the ATM jackpotting problem by providing multiple lines of defense against the ATM attack vectors. This unique approach ensures that the solution can be incrementally extended to account for any new ATM vulnerabilities. Sentient also ends up becoming the one framework on which the next solutions can be built as the next wave of ATM attacks come to light.

Sentient protects ATMs in two key ways - first, very importantly to stop dispensation of cash when an attack is detected, and second, to notify the Security Operations Center (SOC) staff that a suspected attack is in progress; this staff can then notify law enforcement or follow the mandated security procedures.

Sentient provides security for ATMs at multiple layers:

-  **Hard Disk removal detection and remediation** 
-  **Reboot attempt of suspect ATM** 
-  **Antivirus tamper detection and protection** 
-  **Sentient tamper detection** 

Here's how Sentient provides security for ATM's at each layer -

- **Hard Disk removal detection and remediation**
 - Detects removal of the hard disk
 - Sends a critical alert to the SOC and marks the ATM to be in a suspicious state
 - Triggers ATM shutdown
- **Reboot attempt of suspect ATM**
 - Detects ATM under suspicion since the previous hard disk alert
 - Triggers ATM shutdown on each reboot attempt until the alert is cleared
- **Antivirus tamper detection and protection**
 - Detects tampering with antivirus
 - Reboots the ATM each time it comes up
 - Continues rebooting until the antivirus is restored
- **Sentient tamper detection**
 - Alert on Sentient servers due to a number of lost heartbeats from ATM
 - Detect antivirus tampering with client scripts
 - Reboots the ATM each time it comes up



Sentient enables checks at hardware layer and BIOS to ensure ATM integrity. The solution also adds advanced checks for missing services/processes, missing or tampered files, unusual patterns of cash dispensation that are not possible through human interaction with an ATM to make this a futureproof prevention and protection solution.

6 Summary

ATM jackpotting and many other cyber-crimes like these are likely not to go away. Every indication and forecast are that the society should only expect them to increase. Given this reality, and the real cost of damage through ATM Jackpotting, it behooves financial institutions to find solutions that mitigate this growing scourge.

Sentient is that one solution that addresses the ATM Jackpotting problem today, with the assurance of taking care of the next vulnerability or attack - without having to deploy yet another point solution.

About Accelerite

Accelerite is a Silicon Valley based company delivering secure business-critical infrastructure software for Global 1000 enterprises. Accelerite's product suite includes hybrid cloud infrastructure, endpoint security, big data analytics, and the Internet of Things.

To know more about Accelerite Sentient, visit: www.accelerite.com/sentient