Safeguarding Banks Against ATM Jackpotting!

Accelerite Sentient - Industry leading ATM Jackpotting solution

ATM jackpotting is a sophisticated cyber-crime where hackers take control of the ATM's computer allowing them to take out cash on demand. The malware introduced by the hackers interacts with the ATM's software and hardware, making it relatively easy to dispense cash. ATM Jackpotting has affected Europe, Asia and now US.

Sentient is an extensible security framework that mitigates the ATM Jackpotting problem by creating impenetrable lines of defense, with instant tampering alert, trigger of halting cash flow and constructing a dead-end by shutting down the ATM.

This unique approach ensures that the solution can be incrementally extended to account for any new ATM vulnerabilities. Sentient protects ATMs in two key ways - first, 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; the staff can then notify law enforcement or follow the mandated security procedures.

It's crucial today more than ever to explore probable mitigation mechanisms to safeguard yourself against ATM Jackpotting before it is too late.

How Sentient Secures ATMs at Each Layer

Disk removal detection and remediation

- **Detects** removal of hard disk
- **Sends a critical alert** to Sentient server
- **Triggers ATM shutdown** over and over until the alert is downgraded

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 downgraded

Antivirus tamper detection and protection

- **Detects** tampering of antivirus
- **Reboots** the ATM each time it comes up
- **Continues Rebooting** untill the antivirus is restored

Sentient tamper detection

- **Alert on Sentient Server** due to a number of "lost heartbeats" from ATM
- **Detect antivirus tampering** with client scripts
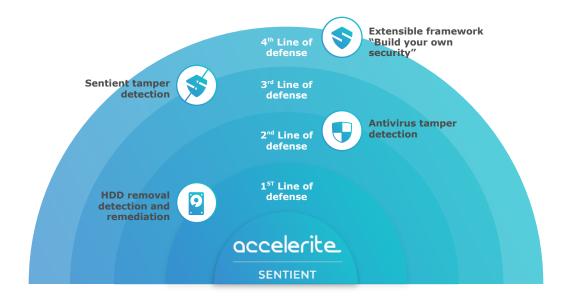- **Reboots** the ATM each time it comes up

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

Vendor Independent ATM Jackpotting Solution

DIEBOLD NIXDORF   NCR   HYOSUNG

4th Line of defense — Extensible framework "Build your own security"

Sentient tamper detection

3rd Line of defense

2nd Line of defense — Antivirus tamper detection

HDD removal detection and remediation

1ST Line of defense

accelerite

SENTIENT

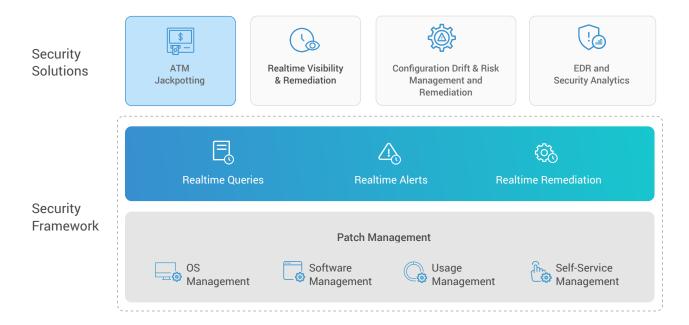## Jackpot Detection & Prevention Use Cases

- Attacker removed the hard drive

- Attacker unplugged the dispenser or USB hub

- Attacker stopped a critical service or process from running

- Attacker renamed a directory (or deleted it) containing critical software

- Attacker unplugged the network interface cable from the ATM

- The dispenser puts out more than X notes in Y seconds

- Dispense occurs without a card being present

Why Sentient ATM Jackpotting solution?

- Vendor neutral ATM security

- IoT architecture ensures scale and performance

- Integration into SIEM for seamless fit into existing infrastructure

- Extensibility to combat new attack vectors

- Tool consolidation on your ATMs

Managing multiple security tools across multiple geographies with diverse platforms is challenging and inefficient. With limited budgets and resources, CSOs and teams want easy to manage technologies that can integrate with each other to improve overall security. Sentient's ATM Jackpotting solution comes with a built-in extensible security framework on which additional security solutions can be built to prevent future breaches. It is the only proactive solution that can not only remediate today's attacks but also build the foundation for tomorrow.

Extensible Sentient Security Framework

Security Solutions

| ATM Jackpotting | Realtime Visibility & Remediation | Configuration Drift & Risk Management and Remediation | EDR and Security Analytics |

Security Framework

Realtime Queries   Realtime Alerts   Realtime Remediation

Patch Management

OS Management   Software Management   Usage Management   Self-Service Management

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, risk based authentication, endpoint security, big data analytics, and the Internet of Things.

Learn more at: accelerite.com/sentient