SECURE YOUR EVERYTHING™

CHECK POINT
ATM Security Model
Powered by Quantum Spark

> “Quantum Spark gateways are easy to use, although there is complexity under the hood.”
>
> Check Point customer using Quantum Spark gateways securing their ATMs

INSIGHTS

Automated teller machines, ATMs are targets for a variety of attacks. Criminals are always looking to use new methods attacking these solutions. Attacks vary from physical attacks to sophisticated Cyber Security attacks. Therefore, ATMs must be protected and secured with dedicated security controls, tailored to their specific needs and requirements.

INTRODUCTION

Taking a look at the attacks performed on ATMs we distinguish three categories: physical, logical and identity targeted attacks.*

Physical attacks are all about stealing cash and hardware assets from the ATM.

Facts | Gas and explosive attacks represent 52% of all physical incidents. 42% is about ram-raid attacks and to 2% is addressed by vandalism.

Attack examples | use of explosives, gas, cutting devices, drilling machines and ram-raid attacks. With ram-raid attacks vehicles are used to penetrate the ATM for looting of cash. We also see sensor tampering for taking out cash without debiting, called forking attacks.

Logical attacks are all attacks that are not physical. Think of Black Box attacks (started initially as physical attack) and malware family types targeted for the ATM or the ATM’s network.

Facts | 74% of all reported logical attacks were Black Box attacks

Attack examples | about 90% of all ATMs worldwide are still running Windows XP. We see attacks trying to exploit vulnerabilities of this outdated OS. We also see “Jackpotting”, inserting malware on the ATMs hard disk to control the cash dispenser. The majority of logical attacks are Black box attacks. This is done by adding an device on the dispenser to bypass the need for cards and authorization. There are over 20 ATM family malware types. The most notorious one is Ploutus. Ploutus is a very sophisticated malware family that allows criminals to empty the ATMs cash cassettes, “Jackpotting”. This done by exploiting ATM XFS middleware vulnerabilities via an externally connected device.

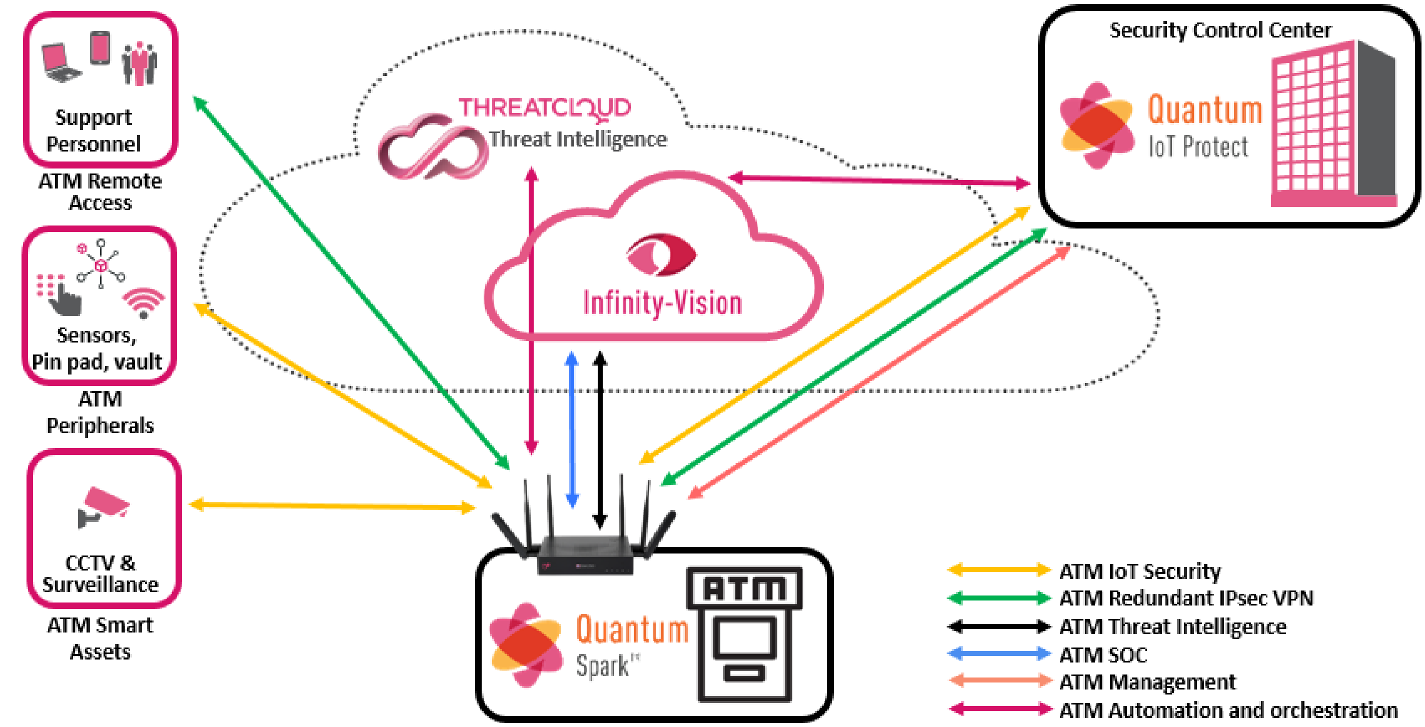
Identity theft is about pin pad tampering, skimming, shimming, card trapping and card sniffing. All methods to captures authentication data for financial gain by reading and capturing data from the cards microchip. Identity theft can also be done via sniffing attacks and eavesdropping.

Facts | 24% is terminal related fraud attacks

Attack examples | Skimming is done by adding a device on the card reader to copy or clone the card. Shimming is another method for intercepting and manipulating data from and to the card microchip.

A BETTER APPROACH TO SECURING ATM ENVIRONMENTS

ATMs require a proactive security solution approach. Examples for security measurements are securing data traffic using IPsec VPNs providing in addition authentication and authorization at central sites. In addition, security for IP cameras used for surveillance and smart sensors observing physical attacks must be provided. Network security systems are preventing unknown and known attacks, securing vulnerable ATM systems from being exploited. The solution should provide insights and visibility with ATM specific alerting. Those events should be shared with a SIEM solution and turned into actionable alerts. The above listed measurements are making sure the ATM attack surface is not increased when adding surveillance and security assets.



ATM PROTECTION - POWERED BY QUANTUM SPARK

Check Point Quantum Spark secures the ATM environment: A dedicated security solution also suitable for smart lockers, smart vending machines and similar solutions. The Quantum Spark security gateway benefits from Threat Intelligen ce provided by Check Point ThreatCloud preventing known and unknown attacks against that logic of the ATM s ystem. It provides redundant IPsec VPN connections to the ATM control center, supporting dual 4G LTE (5G LTE is on our roadmap) connectivity as well as WAN and DSL connections. The Check Point IoT control functionality provides security for smart assets such as surveillance cameras and sensors. Security policies and VPN connectivity are managed by Check Point Infinity Unified Management platform. Scale is achieved by using easy deployment, provisioning and SmartLSM components providing template based device and security settings. Security events are visualized using the SmartEvent and Check Point Infinity SoC (a cloud-based threat hunting platform). This enables security experts to investigate and shut down attacks faster.

CONCLUSION

The finance industry is challenged by the growing attack surface of their ATM environment, exposed to a rapid evolving threat landscape that varies from physical to cyberattacks. All communication with ATM devices must be encrypted and secured with appropriate security controls. ATMs operating system, the cameras and sensors providing physical security, must be protected from known and unknown attacks. Check Point Quantum Spark security gateway for ATM provides zero-day threat prevention, IoT asset and security management and centralized control by the Infinity Unified Management platform.

* **Source** | E.A.S.T https://www.association-secure-transactions.eu/east-presents-on-atm-attacks-at-eufcc/