Integrated Sensory Constructure Unit

American Financial Industrial Teller Security

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Integrated Sensory Constructure Unit

American Financial Industrial Teller Security

Overview

Major attacks attributed to the North Korean Lazarus group, **where the** primary goal of an attack was monetary, executed by installing malware which would then trigger a malfunction command in the software to distribute money the black box mechanism used in ATMs.

These attacks would classified as logical and supply chain attacks, which were spearheaded by infecting the systems utility with malware.

Black box malware attacks were a second generation cyberattack to card skimming which had fallen significantly with the introduction of black box malware phishing.

Integrated Sensory Constructure Unit

Reconstructing all physical teller machines with a base shell that is reinforced and intertwined with sensory cables within the infrastructure. The sensory cables would be an essential aspect of the overall constructure integrity of the machines, which would notify a security agent if tampered or alter in any way.

The counter space and buttons would require built-in scanners which would activate a digital capture which could retrieve fingerprints and the constructure sensory system would notify task force.

Impersonation of technician with the purpose to withdraw can be prevented by encoding uniforms with primary identification codes and phantom codes, as mentioned in previous assignment that counter-syncs, records maintenance work and sends reports to security and manageable after the completion of each worksite.

The uniforms would be reimagined with unique coloring for added security and defense of the detection of imposters by unique colors, which activate a high-security responses. This helps protect the technicians as well.

Detection of digital devices within close range: logs, identified and classifies security risk. In the case of laptops within close range, would signal an alarm to both user and security system. This would as prompt the system to ask for additional security information to verify the identity.

Software engineered for rapid and continuous loop system checks after, during, and before each transaction assuring the integrity of security system. This system would assist in the isolating attacks by early detection and swift retrieval of information regarding attacks.

Reversing attack: Defense: upgrading sensory detection on USB ports and any vulnerable ports on machines which swipes the machines identifications to the security center and signals an alarm system.

A locking mechanism arrest devices in place, making attackers unable to retrieve their devices.

This defense system would also install remote malware and phishing software to send the attackers data to law enforcement with the goal of compromising cybercriminals enterprises and their associates.

Anonemis Research
Simenona Martinez
AnonemisResearch.com