# Insider threat – the Card Shark

## 2018 Data Breach Digest

verizon

### The situation

Despite seeing most attacks coming from outside sources (e.g., hacking, spear phishing, etc.), occasionally we see attacks emanating from within a victim organization's own network environment.

One such case involved payment card data compromise involving unauthorized automated teller machine (ATM) withdrawals resulting in significant financial loss. For this case, we – the VTRAC | Investigative Response Team – were engaged to conduct a Payment Card Industry (PCI) forensic investigation.

### Investigative response

After arriving onsite, the first thing we noticed was that we were granted immediate access with no security or identification checks. This was unexpected and unusual, considering the circumstances. We were also informed that most of the staff who we wished to interview had been replaced due to the incident and that the new staff were still becoming familiar with the environment.

Our initial security information and event management (SIEM) log analysis identified a malicious system within their environment. This system was neither corporate-owned nor "known" which raised multiple questions, including how the system made its way onto the network, where it was located, how it gained access into the PCI environment and why no one noticed the initial alerts.

### Detection tips

- Properly configure network security monitoring software (e.g., SIEM, Intrusion Detection System (IDS)) based on use cases; regularly review outputs and events
- Train employees on cybersecurity policies and procedures, and in doing so, sensitize them to report suspicious cybersecurity and physical security incidents

All we had to go on was a rogue system connected to the network and indications that it accessed critical PCI server databases and conducted unauthorized withdrawals. We still didn't know how the system came to be on the network or exactly how the attack occurred, so we focused in on gathering further information.

We set about conducting interviews and collecting technical information, such as the network topology, to fully scope out the incident and identify possible intrusion vectors. The insight provided by this additional information revealed the entire network structure was flawed from the ground up.

Despite a few internal firewalls, the network was essentially flat. In addition, full network access was available to any connected device due to the lack of even rudimentary access controls. In-place network monitoring was not correctly configured, and while there was a SIEM in place no one was reviewing and investigating alerts.

These fundamental design flaws in the entire network weren't only an open door for attack, but also made it trivial for a threat actor to fly under the proverbial radar.

We reviewed the physical security controls at the location where the attacker's system was determined to have connected during the attack. The location was a main data center, which was a large office building with a publicly accessible area.

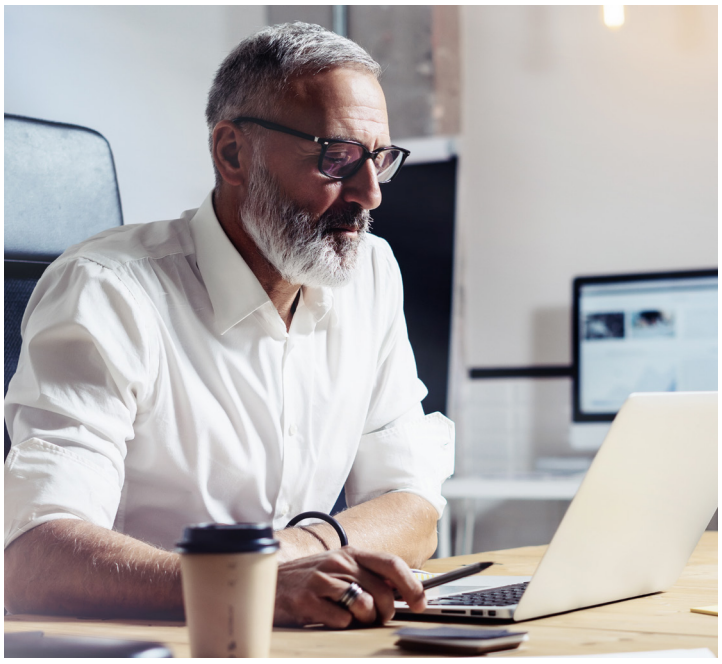
To our surprise, the data center's access was secured only with a standard keyed door. Once inside, all offices were easily accessible. This lax security posture included no identification verification, no access control lists, and no one consistently occupying the security desks. We quickly realized that accessing the employee areas from the public areas would've been relatively easy due to the weak physical security.

Besides the poor physical security, we identified major flaws in the organization's digital security posture. These flaws included easily guessable passwords, unchanged admin account passwords, shared user and admin accounts, database access by default user accounts, and admin privileges for every database user account.

Forensic analysis revealed an attacker with physical access used the suspect system to gain access to one of the application servers via an admin account. The attacker generated scripts to manipulate the database and executed these on the night of the incident. Unfortunately, the suspect system was never found and therefore was not available for analysis.

### Mitigation tips

- Restrict physical access: employ physical security measures, such as identity cards, card swipes, and turn-stiles; further restrict access to sensitive areas
- Restrict logical access: segment the network; prevent rogue system connection to the network; implement multi-factor authentication; use complex passwords for all user accounts



## Lessons learned

In the end it was obvious what lead to the compromise:

**Step 1: Gain physical access**
Weak physical security controls allowed the attacker to gain physical access and introduce an unauthorized system to the organization's premises.

↓

**Step 2: Obtain logical access**
Insufficient network access controls and poor network segmentation enabled the attacker to connect to the internal network and access critical server and database systems.

↓

**Step 3: Leverage privileged access**
Weak password policies enabled the attacker to logon with admin privileges and manipulate the target databases to complete the attack.

Figure 1. The anatomy of the attack

Finally, the lack of proper utilization of network monitoring prevented the organization from detecting this attacker at an early stage.

Not known at the end of this investigation was to what level the attacker had "insider" support. Potential answers for many of our questions vanished with the undiscovered suspected system.

### Detection and response

- Properly configure network security monitoring software (e.g., SIEM, Intrusion Detection System (IDS)) based on use cases; regularly review outputs and events
- Train employees on cybersecurity policies and procedures, and in doing so, sensitize them to report suspicious cybersecurity and physical security incidents

### Mitigation and prevention

- Restrict physical access: Employ physical security measures, such as identity cards, card swipes, and turn-stiles; further restrict access to sensitive areas
- Restrict logical access: Segment the network; prevent rogue system connection to the network; implement multi-factor authentication; use complex passwords for all user accounts