FireEye™

Threat Landscape: **Retail Industry**

Learn More at the **Retail Security** webpage

Clean Up on Aisle Four: How Attackers Exploit Retailers' Networks for Financial Gain

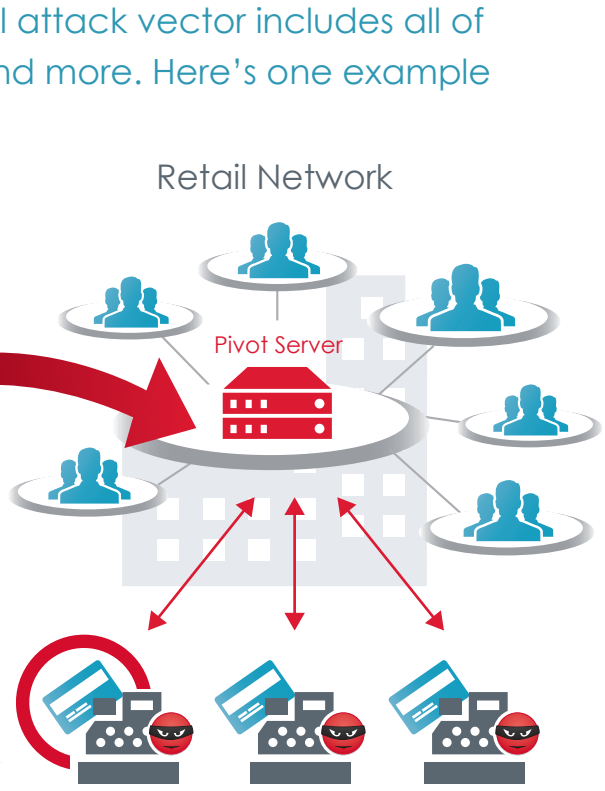
Retailers are a favorite target for cybercriminals. Credit card data is a lucrative asset and can be quickly monetized. High-traffic periods such as the holiday shopping season encourage attackers to invest in schemes that can be reused across multiple retailers for maximum profit.

How Do Attackers Get In?

Attackers invest in elaborate schemes to compromise retailers. The initial attack vector includes all of the usual suspects: spear phishing, drive-by downloads, SQL injection, and more. Here's one example that Mandiant, a FireEye company, saw in a recent investigation.

1 Attacker compromises third-party vendor using spear-phishing email and leverages site-to-site VPN tunnel and compromises retailer.

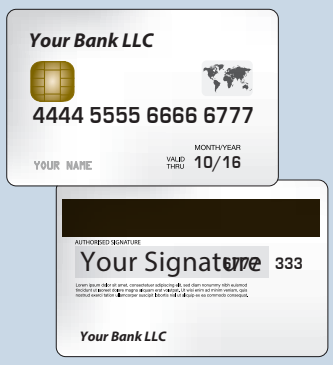
Third-Party Vendor



2 A domain controller, which provided authentication for corporate offices and retail stores, provided the vulnerable pivot point.

What Are They After?

Attackers target Windows-based point of sale (POS) terminals, controllers, and servers. Their ultimate goal is to steal the track 1 and track 2 data stored in the magnetic strips of cards to create counterfeits.



3

The card-harvesting malware deployed on each register searched the process memory of the POS application for magnetic stripe data stored in ISO/IEC 7813 track 1 and track 2 formats.

Track 1 & Track 2 Data:
Contains the primary account number, expiration date, and cardholder name, among other data.

Latest Fashions in Cybercrime?

Attackers are constantly innovating. Here are two new attack vectors that FireEye has witnessed recently.

POS Access

Attackers used minor misconfigurations in the infrastructure to find systems with direct access to the POS systems.

Buying Botnets

Threat actors gained access to systems previously compromised and infected by a botnet herder.

WHAT CAN YOU DO?

Manage Privileged Accounts
Each system in your PCI environment should have its own unique local administrator password. Employ the principle of "least privilege" to all account and group permissions, including the service accounts.

Encrypt Cardholder Data
Consider a POS solution with end-to-end asymmetric encryption, starting at the PIN pad reader.

Actively Monitor
Monitor your PCI environment regularly for abnormal activity, such as suspicious logons, creation of unexpected files, or unusual traffic flow.

Segment Networks
Separate any system that handles cardholder data from the rest of your corporate environment. Require two-factor authentication for access to the PCI environment.

Secure Endpoints
Ensure that all critical systems in the environment implement application whitelisting. Patch all third-party applications and operating systems, and consider implementing a file-monitoring solution that tracks when files have been created on a system.