illusive

Retail Industry Under Attack

What do attackers want?

The global retail industry makes an estimated $20 trillion in sales per year. This is made possible by a high availability of retail services and the ability to manage billions of dollars in digital, credit card based transactions.

This makes the retail industry prone to attacks that either threaten operational uptime or target customers' financial data, which flows in abundance across each network.

Why do attackers target Retail?

These sales numbers are due, in part, to retail services' constant availability. Attackers know that a minute of downtime will cost some retail organizations millions, so they execute denial of service (DOS) attacks at crucial times to demand hefty ransoms.

The large annual sales revenue is also due to billions of dollars in digital transactions that use methods such as credit cards. Attackers target this information for high-frequency, low-reward theft.

What is the risk?

Attacks that cause downtime, targeting a retailer's core system or customer gateway (website, mobile application, etc.) result in serious financial loses that worsen by the minute.

Additionally, attacks that compromise customers' financial data wreak havoc on a company. Having credit card information stolen from your network can result in financial losses, having your PCI compliance revoked, customer and third party lawsuits, and possibly regulatory fines. In addition, retail data breaches often have long-term effects on brand reputation.

How do attacks operate?

As customer experience is key in the retail industry, networks are primarily designed to support the most efficient customer journey from entry to checkout, sometimes at the cost of IT security.

Cybercriminals are sophisticated, organized, and well resourced. Targeting your network for entry points, they will find a way in. Once inside, attackers diligently explore the network via lateral movements, seeking service-critical machines and hosts that store sensitive information.

When a target host is found, attackers generally either steal financial information, exfiltrate your sensitive data and sell it, or run ransomware processes and compromise the availability of your service.

What are the challenges to protection?

- Making your service scalable means providing easy external access and transaction processing (via POS). Sensitive data flows across your network, from many locations, even though you have PCI compliance. For this reason, your network will always be a targeted.
- Staying competitive involves immediately supporting the services that customers adopt. Legacy systems, which fall short of modern security standards, are often speedily patched to newer technologies that enable external access and exploitation.
- Keeping services available 24/7 requires distributing access, and security, through multiple channels (local stores, websites, mobile applications). Distributed security, and the challenges of patching local resources in physical stores, creates cracks in IT defense that attackers creep through.

What would minimize the risk?

With so many attack vectors, bad actors will always find a way onto your network. Risks are minimized by restricting attacker movements, feeding attackers false information, and blocking ransomware processes from real data.

With illusive's agentless solution installed, you can detect access attempts with high fidelity and identify attack tools via real time, source-based forensics. The Advanced Ransomware Guard™ deception family specifically blocks ransomware processes. To gain better optics into your network, illusive networks Attacker View™ offers visibility into large networks and identifies discoverable attack-vectors.