White Paper

THE FOUR ATTACK VECTORS TO PREVENT OR DETECT RETAILER BREACHES

By James Christiansen, VP, Information Risk Management

ACCUVANT

Executive Summary

Security breaches in the retail sector are becoming more commonplace due to the large payoff to criminals in seizing digital information. While many companies are focused on anti-malware for point of sale (POS) systems, it's important to understand and remediate the different vectors that an attacker may use to gain access to the POS or corporate systems. Understanding the patterns and profiles provides a method to prevent or detect the attacks as they are occurring. While this paper focuses on the retail sector, these types of attacks can occur in any industry sector that holds sensitive data, such as healthcare records or intellectual property.

How a Malicious Attack Happens

Many large companies allow third-party vendors to have access on their corporate networks to automate their key business-to-business (B2B) processes. Providing third-party vendor access to systems and processes, however, may increase the probability of being attacked and pose potential security risks. In many cases, data sent between the third-party vendor and the company corporate network may seem harmless, but this connection may be a point of attack.

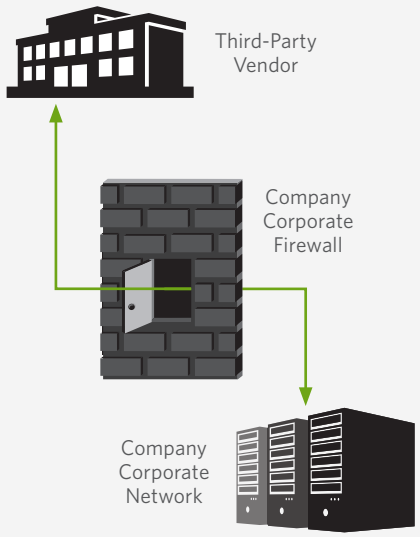


Figure 1: Typical external third-party vendor access.

While a contract may be in place between the third-party vendor and company to ensure the vendor has proper security measures in place, this might not be enough to ensure the corporate network and systems are secure. Accuvant recommends implementing a robust third-party risk management program to prevent intrusions.

An attacker's ultimate goal is to gain access to sensitive information both in the corporate network and the POS systems. If an attacker focuses on a trusted third-party vendor, they may gain login credentials that will allow access to the company's corporate environment. These trusted third-party vendors may not deploy as stringent of controls as the corporate network. Thus, the attacker may find an easier attack path through the vendor network rather than trying to directly break into the corporate network.

Often, a phishing attack is launched at the third-party vendor to gain valid login credentials for the corporate network. Emails that appear to be from a friend, family member or colleague suggest the recipient click on a link that will appear legitimate, but it is actually a site that infects the computer with malware. There are many examples of increasingly sophisticated phishing attacks using embedded links that place malware on the unsuspecting reader (figure 2).

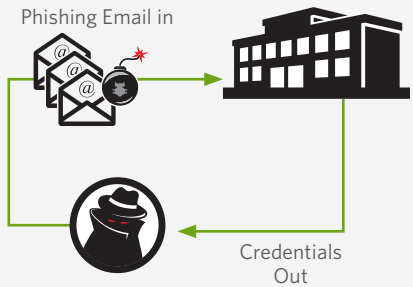


Figure 2: Attacker attempts to get access to third-party network.

If the attacker succeeds in gaining valid login credentials through the phishing attack, they can use those credentials to access the company's corporate systems. Since the attacker has valid login credentials, the corporate security system will not recognize this as an attack.

Once the attacker has signed into the company's corporate application system, they can use common attack methods to escalate privileges (figure 3). Most attacks can be prevented by using secure coding techniques for websites, such as those recommended by the OWASP community, and maintain systems with an effective vulnerability management process. A thorough application penetration testing process will discover many of the potential vulnerabilities that an attacker would use to escalate their privileges. Though not all zero-day attacks can be prevented, they can be detected early with proper monitoring before any major damage is done.

Once the attacker has privileged access on the network, they can begin to move laterally across the internal network, seeking systems and data of opportunity (figure 4). A sophisticated attacker will move slowly across the network to avoid being detected by intrusion detection software (IDS) and security event monitoring. There are many products commercially available in the market that can identify these slow moving attacks and send alerts to the security staff.

In today's corporations, there are many attack alerts that may possibly overwhelm the staff's ability to react to them all. Companies must implement and maintain Security Information and Event Management (SIEM), define events of interest (EOI) and train staff to assess whether the EOI poses a serious threat. Ignoring an alert is like driving a car with the check engine light on because there are seemingly no other symptoms of a serious problem.

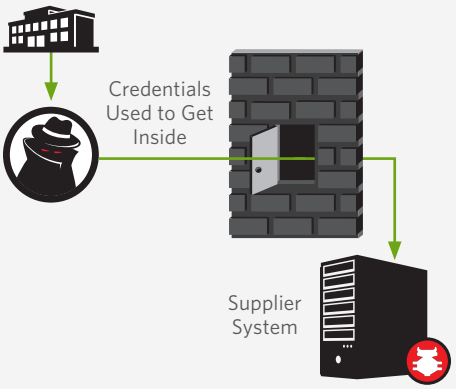


Figure 3: Attacker gains access to the third-party supplier system in the company's corporate network.

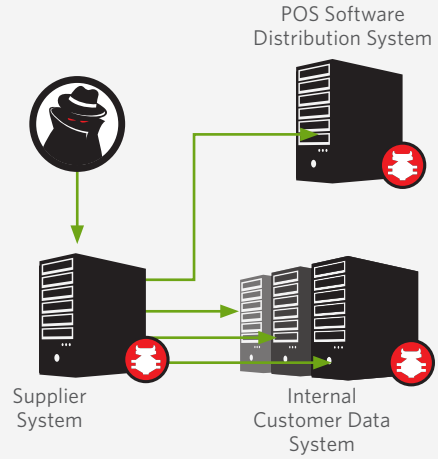


Figure 4: Attacker escalates privileges and begins to move laterally across network.

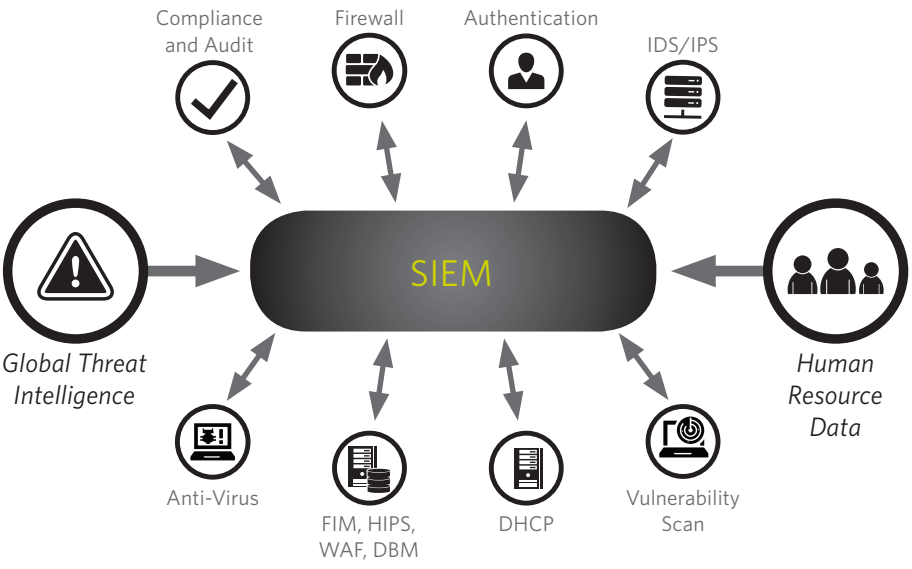


Figure 5: Sample of how SIEM may be configured on a corporate network.

As the attacker moves laterally across the internal systems, a popular prize is gaining access to the software distribution system that manages the POS devices. Once the attacker attains access to the software distribution system, malware can be inserted into a run-time package and distributed to each of the POS systems. The attacker has effectively used the organization's own management and automation tools to quickly and inconspicuously infect potentially thousands of POS systems. Since the new code has been authorized by the software distribution system, any anti-malware system on the POS device will see the code as whitelisted (figure 6), therefore rendering its defenses useless.

The malware used in recent retailer attacks was designed to search through memory for credit card information in cleartext and then write the information to a small file on the POS system. Even if the POS system was designed to only write credit card information to an encrypted file, the malware has successfully written the sensitive information into a different file that it controls, which might have its own encryption to avoid detection.

Most POS networks establish two or three separate security zones. The POS network zone isolates the POS systems from the back office systems, such as supply chain management or enterprise resource management. A third network zone may be defined so the retailer can offer Internet service to guests. The network isolation presents a problem to the attacker trying to exfiltrate their stolen information. Sending data directly out of the retail store to a server on the Internet would be easily prevented and detected. It is more likely that the attacker will disguise the files and transmit them back to the host system where the attacker has an established a foothold (figure 7).

While the data is accumulated from the POS systems, the attacker will continue to search for sensitive information across the host systems. If an attacker discovers databases that contain sensitive customer profile information, the malware, sitting quietly on the network, will move this data into a hidden database that the attacker can access at any time (figure 8).

The attacker may move the hidden database files to an unprotected and unmonitored server to begin the exfiltration process, moving the data out of the organization's network to external servers for which they have anonymous access (figure 9).

Once the cardholder information and customer data has been moved to the external servers, the attacker will move the data to their own systems, completing the loop. The card data can then be sold on the black market for quick cash and the consumer information can be used to create broader and more sophisticated phishing attacks.

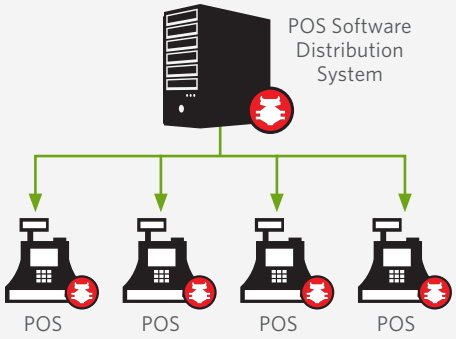


Figure 6: POS devices are infected with malware.

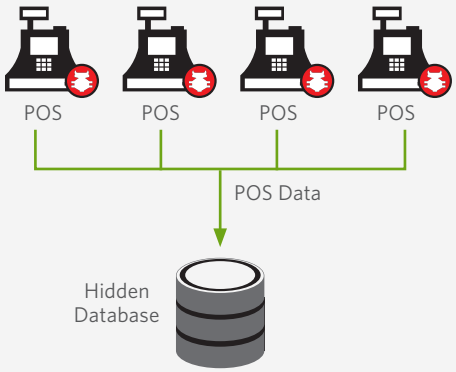


Figure 7: POS data is stored in hidden database.

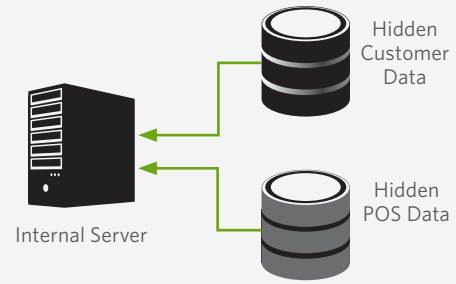


Figure 8: POS and customer data is moved to an internal server.

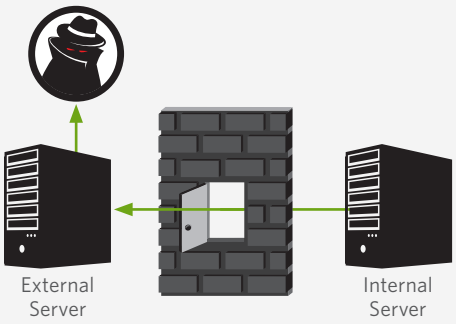


Figure 9: Data is exfiltrated in pieces to an external server

How to Prevent and Detect a Retail Attack

In the scenario above, there are four primary points of the attack. The attack could have been stopped if the proper people, processes and technology were in place.

Attack Point One

The phishing attack on the retail third-party vendor could have been prevented by having a commercial anti-malware program and an effective security awareness program such as an anti-phishing policy. Train employees to recognize and report cases of suspected phishing emails to their security departments. Organizations should implement a comprehensive third-party risk management system to complete reviews of their vendor's security controls.

Attack Point Two

The successful attack on the third-party portal could have been prevented with a combination of secure coding practices, active vulnerability management, application penetration testing, and separate network security zones.

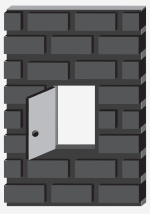
The attack against the software portal and attacks against the other internal systems should have been detected with alerts created by the SIEM. Trained security staff along with effective processes are required to react to the alerts and contain the attack before sensitive data can be exfiltrated.

Attack Point Three

The POS systems should always have a commercial anti-malware system that is kept current with the latest threat information. In an attack scenario, the malware may be whitelisted and the anti-malware system will not identify it. Anomaly detection software can alert the security team that unknown files are being created and transmitted out of the environment. Good network protection practices are required to keep attackers from directly accessing the POS systems, either directly from the Internet or from within the physical retail store.

Attack Point Four

As the POS and consumer data are being accumulated on the internal servers and exfiltrated out of the network to the external servers, an anomaly-based intrusion detection system identifies the files being moved and sends alerts to the security team. If the data being exfiltrated is not encrypted, then a properly configured data leakage prevention system can analyze and detect network traffic for social security numbers, credit cards or other critical data content.



In summary, several key security initiatives that can significantly reduce the risk of an attack in a retail setting include:

- Install and maintain commercial anti-malware protection.
- Perform application penetration testing.
- Train application development staff on secure coding techniques.
- Implement a vulnerability management program.
- Ensure that security event monitoring captures and reports critical security alerts and that staff is ready to react to the alerts.
- Have a trained and tested incident response team.

Final Thoughts

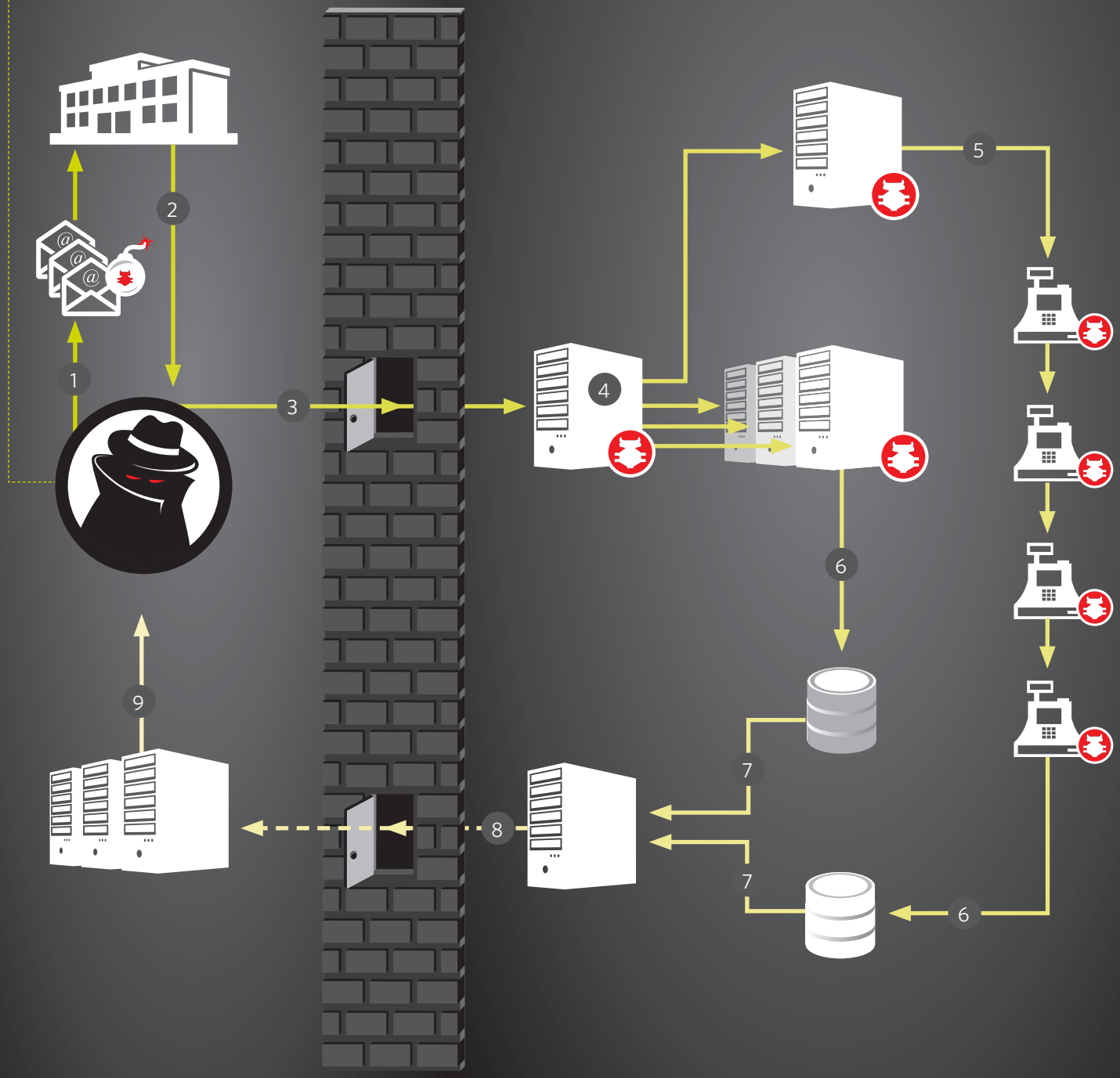
There are a variety of techniques that an attacker uses to gain access to sensitive information and exfiltrate the data outside of the retailer's network. A holistic approach takes a broad perspective of your corporate system, processes and the people in the environment.

Third-party risk management is garnering much needed attention as a source of attack as is POS device security. However, while recent attacks are using advanced malware and phishing, a key component missing in the conversation are the sophisticated evasion, delivery and exfiltration techniques that are undetected or ignored in the victim's own environment. What appears to be an "insider threat" is not a malicious or negligent employee; it is an attacker that has the credentials and controls to behave like an insider.

Focus has been on the retail sector due to recent breaches, but a similar breach could happen in almost any business. An attacker may pursue credit card data, healthcare records or intellectual property. It is essential to implement a holistic security strategy plan to protect your corporate assets. This starts with mapping out all possible internal and external threat scenarios in your environment and using a third-party security expert to assess your infrastructure.

DIAGRAM OF A RETAIL ATTACK

1: Phishing email sent to third-party vendor. 2: Credentials out. 3: Attacker gains access to the third-party supplier system in the company's corporate network. 4: Attacker escalates privileges and begins to move laterally across network. 5: POS devices are infected with malware. 6: POS and Customer data is stored in hidden databases. 7: POS and customer data is moved to an internal server. 8: Data is exfiltrated in pieces to an external server. 9: Attacker moves data to their own system, completing the loop.



Accuvant, a Blackstone (NYSE: BX) portfolio company, is the leading provider of information security services and solutions serving enterprise-class organizations across North America. The company offers a full suite of service capabilities to help businesses, governments and educational institutions define their security strategies, identify and remediate threats and risks, select and deploy the right technology, and achieve operational readiness to protect their organizations from malicious attack. Founded in 2002, Accuvant has been named to the Inc. 500|5000 list of fastest growing companies for the last eight consecutive years. The company is headquartered in Denver, Colo., with offices across the United States and Canada. Further information is available at www.accuvant.com.

BR14 | F1.1

ACCUVANT

1125 17th Street Suite 1700 | Denver, CO 80202
800.574.0896
www.accuvant.com