imperva

DATASHEET

Defending Against Complex Data-centric Attacks

When threat actors attack your IT systems, taking over user accounts and installing malware are some of the key stepping stones, but the real objective is to steal, modify or delete sensitive, valuable information. Application vulnerabilities leave the door open to attacks such as SQL injection (SQLi), consistently reported as the number one attack method by the Open Web Application Security Project (see OWASP Top Ten).

Using SQLi to target databases is not a new threat, but recent news about attacks leveraging weaknesses in trusted vendor software such as Accellion's File Transfer Appliance (FTA) have brought this issue back into focus. In the case of FTA, attackers introduced malware into Accellion's product by targeting its software supply chain. As FTA customers updated to the current version, the malware was used to launch SQLi attacks targeting those organizations' databases and their valuable, sensitive contents. Initially, it was reported that the vulnerabilities were quickly fixed and the attack affected a relatively small number of organizations, but the list continues to grow as more breaches are discovered. Victims include banks, insurance companies, telecom service providers, retailers, law firms and government organizations around the world.

Attackers are becoming more creative. What started as a few vulnerabilities that were quickly patched has evolved into a global extortion effort, where victim organizations' private data is weaponized against them.

A data-centric security layer protects against attacks like the Accellion breach

It's impossible to be sure that the software you depend on is free of vulnerabilities, even when you develop it yourself. In a complex IT environment, any system could be a pathway for external attackers or even insiders to achieve their real objective: getting to your data. Experts agree that the optimal defense is a layered security approach which includes data-centric strategies that focus on protecting the data itself, not simply the network, servers and applications around it.

Organizations may assume that keeping their databases fully patched and using built-in security features, such as data encryption and defined lists of users and authorizations, are enough to protect their data. These are essential but not sufficient to guard against sophisticated attacks like the Accellion scenario. In this type of attack, SQLi can circumvent other controls to access, modify or delete records in the underlying databases, or even access the underlying operating systems of the servers hosting the database services.

The FTA breach began by attacking organizations' web application firewalls, then shifted to SQLi attacks to exfiltrate their customer data. This stolen data, including personal identifiable information (PII), tax information, purchase invoices and other information, has begun to leak online on websites affiliated with ransomware gangs. Some victim organizations have already reported incidents where the attackers extorted money to avoid public release of their data.

When attacks at the network or application level succeed, what protections do you have around your valuable data as a last line of defense?

Imperva focuses on securing your data and all paths to it

Imperva's unique approach to protecting your data encompasses a complete view of both the web application and data layer. Data-centric controls prevent and respond to complex, multi-layer data-oriented attacks like the Accellion breach scenario. Imperva builds on and extends databases' native security capabilities.

- **Get the full risk picture.** Continuously discover and classify you sensitive data enterprise-wide so you know where it is, how much there is, and whether it's protected.
- **Actively monitor data access activity.** Identify any data access behavior that's risky or violates policy, regardless of whether it originates with a network SQL query, a compromised user account or a malicious insider.
- **Identify threats you didn't know about.** Advanced data security analytics use purpose-built algorithms to identify complex behaviors that vary from the norm to help you preempt threats before they become breaches.
- **Automate incident response.** Receive automatic notification of an attack so you can respond quickly. Security analytics provide a clear explanation of the threat and enable immediate initiation of the response process, all from a single platform.
- **Be prepared for future needs.** Retain important audit data spanning multiple years and retrieve it in real-time for accelerated risk and forensic analysis.

Complementing its data-centric security controls, Imperva offers additional Application Security Supply Chain defenses such as Imperva's Web Application Firewall (WAF) and Runtime Application Self Protection (RASP). These add the additional layers to protect all the paths to data.

Your data is safe, wherever it is

Imperva's Sonar protects your entire data estate, whether it's located on premises, in your private cloud, multi-cloud, hybrid or DBaaS environment. It secures structured, unstructured and semi-structured data and can leverage and extend your existing data security investments including database activity monitoring (DAM) solutions.

Learn more about Imperva's approach to data security at **imperva.**com.

Imperva protects the data of over 6,200 customers from cyber attacks through all stages of their digital transformation.