TJX Intruder Had Retailer's Encryption Key

30 March 2007

Not that the culprit necessarily needed it. Data was apparently taken during the card-approval process before it was encrypted. These are among the latest details in what is almost certainly the worst retail data breach ever.

The massive data breach at $16 billion retailer TJX involved someone apparently armed with the chain's encryption key, but it might not have been needed as the cyber-thief was accessing data during the card-approval process before it was encrypted.

These are among the latest details in what is almost certainly the worst retail data breach ever.

In a 10-K filing to the federal SEC (Securities & Exchange Commission), TJX said it didn't know who the intruders were, but it did provide more details about what they say happened that led to the card information of some 46 million consumers to get into unauthorized hands.

The intruder or intruders here apparently planted software in TJX systems to capture data throughout the day and they also engaged in an increasingly popular tactic: post-event cleanup.

That's where intruders spend extra effort cleaning up their tracks—deleting and otherwise tampering with log files, changing clock settings and moving data to hide their movements.

"Due to the technology utilized by the intruder, we are unable to determine the nature or extent of information included in these files. Despite our masking and encryption practices on our Framingham system in 2006, the technology utilized in the computer intrusion during 2006 could have enabled the intruder to steal payment-card data the payment card issuer’s approval process, in which data (including the track 2 data) is transmitted to payment-card issuer’s without encryption," the filing stated. "Further, we believe that the intruder had access to the decryption tool for the encryption software utilized by TJX."

“It’s incomprehensible that what amounts to a computer worm was placed on mission-critical systems at one of the world’s largest retailers and remained there—undiscovered—for 18 months. The scope of the theft is stunning," she said. "My biggest fear is that it lays down a gauntlet for other would-be hackers, subtly daring them to ‘top this one.' It also lays down the gauntlet for other retailers. This could be happening to you right now. PCI compliance and data security do not have obvious return on investment. Neither does paying taxes. But avoiding either can result in irreparable harm.”

The filing also raised questions about whether TJX is going to point the finger at others in the industry when blame is handed out for this breach.

"We rely on commercially available systems, software, tools and monitoring to provide security for processing, transmission and storage of confidential customer information, such as payment card and personal information. We believe that the intruder had access to the decryption algorithm for the encryption software we utilize," the statement read. "The systems currently used for transmission and approval of payment card transactions, and the technology utilized in payment cards themselves, all of which can put payment-card data at risk, are determined and controlled by the payment-card industry, not by us."

The filing also revealed a more-detailed timeline of the incident. TJX officials said they first learned of the situation on Dec. 18, 2006, when "we learned of suspicious software on our computer systems."

Three days later, the filing said, investigators brought in by TJX concluded "there was strong reason to believe that our computer systems had been intruded upon and that an intruder remained on our computer systems."

The filing confirmed that the U.S. Secret Service then asked them to keep the matter confidential because the intruder might be caught if he or she

doesn't know TJX discovered the software.

On Dec. 26 and 27, 2006, "we notified our contracting banks and credit and debit card and check-processing companies of the suspected computer intrusion" and "on Dec. 27, 2006, we first determined that customer information had apparently been stolen from our computer systems."

The retailer said that routine file deletions are making it more difficult to identify exactly what was taken. And the intruder is adding to that challenge.

"The technology used by the intruder has, to date, made it impossible for us to determine the contents of most of the files we believe were stolen in 2006," the filing stated. "We believe that we may never be able to identify much of the information believed stolen."

The company has spent about $5 million in a three-month period dealing with this breach, "which includes costs incurred to investigate and contain the computer intrusion, strengthen computer security and systems, and communicate with customers, as well as technical, legal, and other fees."