Issued 1/3/17

Shopped in Forever 21? There was Bank-Card-Slurping Malware Their Equipment

Clothing chain Forever 21 has admitted a malware infection on its cash registers swiped customer payment card details for most of last year in a statement revealing that from how last year, from April 3 to November 18, hackers were able to harvest the payment card details from point of sale (POS) terminals in its stores.

According to Forever21, the crimeware was present at various times on machines throughout the seven-month period with some machines being infected for most or all of that time. Additionally, Forever 21 said, the malware was able to get into appliances that stored transaction log in the stores so it could potentially access cards read by machines that were not themselves infected. Perhaps most infuriating to victims is the fact that Forever 21 actually had encryption tools installed to secure those sales records from prying eyes, but not running, on the infected machines and log storage systems. "When encryption was off, payment card data was being stored in this log. In a group of stores that were involved in this incident, malware was installed on the log devices that was capable of finding payment card data from the logs, so if encryption was off on a POS device prior to April 3, 2017 and that data was still present in the log file at one of these stores, the malware could have found that data."

The company notes that its online store and its stores outside of the US use different payment systems that were not exposed to the malware. Those who card statements, and report any suspicious activity. Forever 21 said it is working with its payment processors, the developer of the breached POS systems, and law enforcement to further investigate the cyber-break-in.