Malware Infected All Eddie Bauer Stores in U.S., Canada

Author: Brian Krebs

Date Published: August, 18, 2016

https://krebsonsecurity.com/2016/08/malware-infected-all-eddie-bauer-stores-in-u-s-canada/

Clothing store chain Eddie Bauer said today it has detected and removed malicious software from point-of-sale systems at all of its 350+ stores in North America, and that credit and debit cards used at those stores during the first six months of 2016 may have been compromised in the breach. The acknowledgement comes nearly six weeks after KrebsOnSecurity first notified the clothier about a possible intrusion at stores nationwide.

On July 5, 2016, KrebsOnSecurity reached out to Bellevue, Wash., based Eddie Bauer after hearing from several sources who work in fighting fraud at U.S. financial institutions. All of those sources said they'd identified a pattern of fraud on customer cards that had just one thing in common: They were all recently used at some of Eddie Bauer's 350+ locations in the U.S. The sources said the fraud appeared to stretch back to at least January 2016.

A spokesperson for Eddie Bauer at the time said the company was grateful for the outreach but that it hadn't heard any fraud complaints from banks or from the credit card associations.

Earlier today, however, an outside public relations firm circled back on behalf of Eddie Bauer. That person told me Eddie Bauer — working with the FBI and an outside computer forensics firm — had detected and removed card-stealing malware from cash registers at all of its locations in the United States and Canada.

The retailer says it believes the malware was capable of capturing credit and debit card numbers from customer transactions made at all 350 Eddie Bauer stores in the United States and Canada between January 2, 2016 to July 17, 2016. The company emphasized that this breach did not impact purchases made at the company's online store eddiebauer.com.

"While not all transactions during this period were affected, out of an abundance of caution, Eddie Bauer is offering identity protection services to all customers who made purchases or returns during this period," the company said in a press release issued directly after the markets closed in the U.S. today.

Given the volume of point-0f-sale malware attacks on retailers and hospitality firms in recent months, it would be nice if each one of these breach disclosures didn't look and sound exactly the same. For example, in addition to offering customers the predictable and irrelevant credit monitoring services topped with bland assurances that the "security of our customers' information is a top priority," breached entities could offer the cyber defenders of the world just a few details about the attack tools and online staging grounds the intruders used.

That way, other companies could use the information to find out if they are similarly victimized and to stop the bleeding of customer card data as quickly as possible. Eddie Bauer's spokespeople say the company has no intention of publishing these so-called "indicators of compromise," but emphasized that Eddie Bauer worked closely with the FBI and outside security experts.

For more on the importance of IOCs in helping to detect and ultimately stymie cybercrime, check out last Saturday's story about IOCs released by Visa in connection with the recent intrusion at Oracle's MICROS point-of-sale unit. And for the record, I have no information connecting this breach or any other recent POS malware attack with the breach at Oracle's MICROS unit. If that changes, hopefully you'll read about it here first.