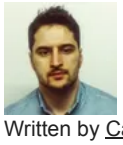
Web skimmers found on the websites of Intersport, Claire's, and Icing

zdnet.com/article/web-skimmers-found-on-the-websites-of-intersport-claires-and-icing/

Home Innovation Security

The malicious code has now been removed from all stores, but users are advised to review card statements for suspicious transactions.



Written by Catalin Cimpanu, Contributor on June 15, 2020

-
-
-
-
-

Security

Everything you need to know about viruses, trojans and malicious software

Cyber attacks and malware are one of the biggest threats on the internet. Learn about the different types of malware - and how to avoid falling victim to attacks.

Read now

Hacker groups that engage in web skimming (also known as Magecart) attacks have breached the web stores of two of the world's biggest retail chains -- accessories store Claire's and sporting goods retailer Intersport.

According to reports published today by security firms Sanguine Security and ESET, hackers breached the two companies' websites and hid malicious code that would record payment card details entered in checkout forms.

Claire's and Icing

According to Sanguine Security's Willem de Groot, the Claire's website was compromised between April 25 and June 13, and so was sister-site Icing.

"The injected code would intercept any customer information that was entered during checkout, and send it to the claires-assets.com server," de Groot wrote today in a report shared with ZDNet, where claires-assets.com was a domain they registered four weeks before for the special purpose of executing this attack.

De Groot said he contacted Claire's management at the time of the attack, and the company removed the malicious code from their site.

Claire and Icing users who shopped online during the above-listed interval are advised to keep an eye out on their card statements for unauthorized transactions and lock their cards and work with their banks if they spot anything suspicious.

"We are working diligently to determine the transactions that were involved so that we can notify those individuals," a Claire's spokesperson told ZDNet today. "Cards used in our retail stores were not affected by this issue. We have also notified the payment card networks and law enforcement. The payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. We regret that this occurred and apologize to our customers for any inconvenience caused."

Intersport

A similar incident was also detailed today by antivirus maker ESET, impacting the website of Intersport, one of Europe's largest sporting goods retail chains, with more than 5,800 stores across the continent.

The skimmer wasn't loaded on all versions of the Intersport website, but only on the local versions serving customers in Croatia, Serbia, Slovenia, Montenegro, and Bosnia and Herzegovina.

According to de Groot, who also looked into the Intersport incident, the company's stores got hacked on April 30, cleaned on May 3, and then hacked again on May 14. ESET said the company removed the malicious code within hours after being notified of the latest hack.

Customers who made purchases on the impacted Intersport websites should contact their card company and monitor statements for fraudulent purchases.

However, In a statement provided to ZDNet and also published on the company's website, Intersport admitted to the incident but said that "no payment card information were intercepted."

Both the Claire's and Intersport incidents took place during the coronavirus (COVID-19) pandemic when most physical stores had been closed, and the companies redirected users toward their online sites for product purchases.

Article updated on June 15, 11:50 am ET with statement from Claire's, and again on June 18, 05:40am with statement from Intersport.

The FBI's most wanted cybercriminals