Luxury Daily®

The News and Intelligence You Need on Luxury

INTERNET

Luxury shopping experience threatened by client-side malware

May 15, 2015

Promotional image for Net-A-Porter premier delivery service; losing just one affluent consumer's purchase has a large impact on a retailer's sales

By SARAH JONES

As more luxury retailers are entering ecommerce, they want to ensure their online storefront fits with their brand image, but without their knowledge, outside factors may be altering the user experience.

Client-side injected malware infecting consumers' browsers may be tampering with the Web page of a retailer, presenting them with pop-ups, product suggestions, fake surveys and ads that are not sanctioned by the brand. These lead the shopper away from the retailer's site, eating into their sales and potentially eroding their integrity.

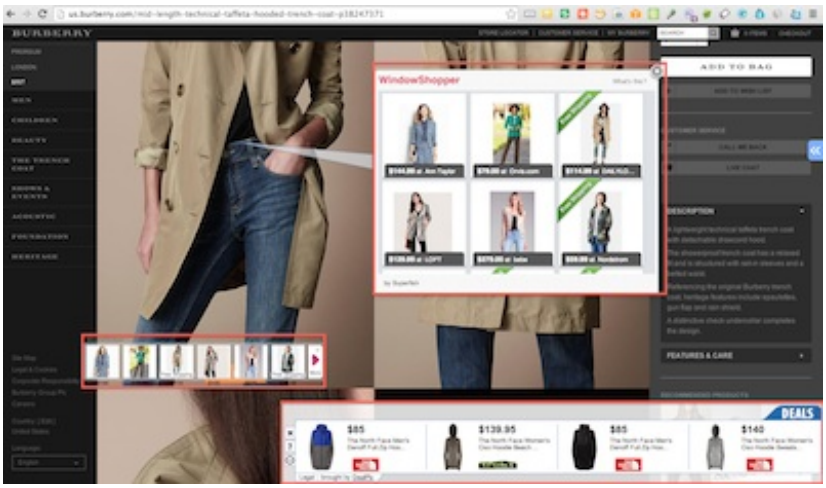
"There's a shift towards online, as we see more and more luxury brands going to ecommerce. It's inevitable they will continue to do so," said Ohad Greenshpan, co-founder of Namogoo, Ra'anana, Israel. "And since there's so much revenue made there, we believe that the problem will become much more significant in the next year or so."

Ecommerce infection

CSIM gets into consumers' computers through extensions installed on their browser or software they did not intend to install, for instance secretly bundled with a program they

decided to download. This can be spyware, widgets or advertisements.

The independent third party then changes how consumers view Web pages, serving up its own ads to make money, without paying the Web site owner or gaining their authorization. These can appear as product suggestions from competitors, which disrupt the Web site's functions; ads, which take users away from the brand site and harm their branding and sales; or spyware scripts, which may prompt consumers to take a fake survey from the brand, allowing a third party to capture proprietary data and hurt consumer trust.



Namogoo capture of malware on Burberry ecommerce site

Typically, iOS devices are thought of as impenetrable, but malware is increasingly targeting these devices with sophisticated operating system-specific extensions that are designed to blend in with the actual site. iOS malware instances have jumped 5 percent to 20 percent over the past six months.

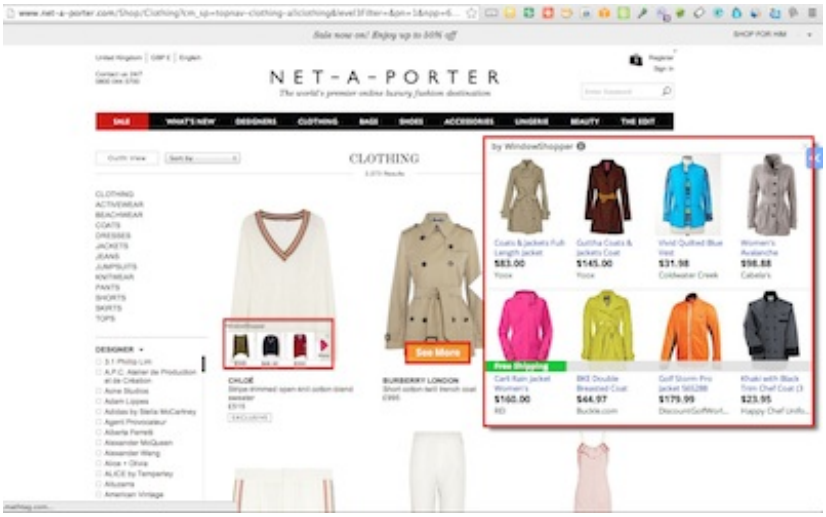
This is particularly important for luxury brands, since 46 percent of luxury site visits come from consumers accessing via iOS devices.

While this is happening on a fairly frequent basis on the consumer side, brands may be unaware of malware, since it occurs on the front end, consumer side.

"From our experience, it's a problem they've never heard of, because they serve the pages as they think they serve them, and then users on their computers have malware of all kind, but they have no way to measure it and to see these pages, and to see it from the eyes of the users," Mr. Greenshpan said. "So they don't imagine that they serve the page one way and the user sees it or experiences it in a different way."

Among luxury brand sites, the incidence of malware is lower than for mass retailers such as Target or Walmart, but the impact can be greater.

Mass retailers see about 15 to 30 percent of their traffic redirected when an experience is injected with malware, while for luxury brands, it is closer to 5 percent. For a luxury retailer such as Net-A-Porter where the average order amount is more than $500, 10 times that of the average, losing just one customer can have more of an effect on revenue.



Namogoo capture of malware on Net-A-Porter's ecommerce site

Traditionally, retailers have not been able to track and prevent malware from appearing. However, security companies like Namogoo are creating technology to protect a site against malware.

Namogoo's servers scan millions of pages daily, placing code on Web sites to block malware in real-time, helping to ensure that a client's Web site is seen the way they intended it.

Protection plan

Recently, luxury brands that have felt imperceptible have suffered other security attacks.

For instance, Neiman Marcus was the victim of credit card theft around the holidays in 2013. Right after, the brand began working to fix security flaws that made the breach possible, but the extent of collateral damage done to its reputation was measured in the following months.

Although the less than 1 million credit cards compromised at Neiman's seems minimal compared to the potentially 110 million affected at Target, consumers are understandably rattled and even outraged, which likely hindered sales. If consumers feel that their credit identity is at risk with every swipe at a major retailer, the damage could take years to mitigate (see story).

Malware also has a part to play in moving counterfeit merchandise, stealing sales from the actual brand.

The fight against counterfeits is a never-ending struggle, exacerbated by the global, online marketplace.

Luxury brands continually seek to win far-reaching court decisions to thwart the capabilities of counterfeiters, only to encounter new opponents and tactics. Now, new technologies are popping up to help brands crowdsource enforcement, but it is still too early to see if they will catch on (see story).

To combat malware, retailers need to integrate a security plan designed to target the various types of software that appears on consumers' devices.

"There is no way to combat this besides working with a service like ours, because once they sell online, they have users, users have malware, these users get more and more malware with installations and bundling that they download, so they will be exposed," Mr. Greenshpan said.

"You could ask the same question about companies that have a security attack, if there's any recommendations besides firewalls to overcome these attacks. That's the solution they should take," he said.

"Because the malware industry is very fragmented, because companies like the ones that develop these extensions are sometimes two or three employees that generate several millions of dollars per month, no legal action can be taken practically. And since this market is so fragmented, we identify at the moment over 25,000 different fingerprints of such viruses, there's no action that can be made to attack this problem on the legal aspect, with regulation."

Final Take
Sarah Jones, editorial assistant on Luxury Daily, New York

Embedded Video: https://www.youtube.com/embed/yRYixVHMXCk