# Home Depot hack shows online card fraud still as easy as shooting fish in a barrel

September 25 2014, by Bill Buchanan


Stolen credit card details, cheaper by the dozen when you buy online. Credit: Chris Young/PA

Imagine if UK banks decided to send out new credit cards to all their customers, but they were all "lost in the post" and the details ended up for sale on some dubious website. The recently discovered hack at huge US firm Home Depot was of that sort of scale – at least 56m credit and debit card details could have been compromised from the company's entire chain of more than 2,000 stores across the US, and others in

Canada, Guam, Mexico and Puerto Rico.

The risk to businesses and individuals from theft of passwords and financial details online is growing. The attack on Home Depot, apparently conducted by installing malware on vulnerable point-of-sale computers, looks bigger even than the attack last year on another huge US retailer, Target, that exposed an estimated 40m card details. It seems that companies have set up a whole lot of back-end defences defending their data, but have forgotten that once the intruder has a touch-point on the network, especially external to their own systems, they can often go undetected.

In one of the largest corporate thefts ever, online auction giant eBay was hacked in May this year, and later admitted that data from all 145m user accounts had been accessed. The intruders managed this by identifying and then compromising the user accounts of senior staff with privileged access to the company's systems. There are clearly significant risks to firms conducting their business on the web, and the importance of keeping a company's crown jewels – its data – safe seems not to have sunk in.

## Faking it on eBay

The site has faced further problems recently from the front end rather than the back. Fake auction listings have been written to take advantage of the site's lax restrictions on the use of HTML and Javascript code in listings, allowing attackers to insert malicious code, known as a cross-site scripting attack (XSS).

Using this and other means to hijack a users' account – perhaps one with 100% positive feedback and hundreds of sales – the attackers use these to set up convincing fake listings containing malicious code that redirects users to convincing pages and prompts them to enter login credentials or

credit card details. These are funnelled off to the attackers, yet all the while the user is unaware than anything untoward is happening. This problem has existed since February 2014.

## Malware scam

It's likely that the malware used to obtain card details from Home Depot ran from April 2014 to the beginning of September 2014 before it was finally detected. It's now been found and removed, but that's no consolation for customers who have already been affected.

The lesson learned must be to reduce the time it takes to detect a threat and to respond quickly. As the back-end of financial services become more secure, hackers will focus more on point-of-sale computers or other front-ends such as websites, so retailers need to spend more effort and resources in proactively detecting exploits and vulnerabilities, as much as they do on data protection.

This breach is expected to cost Home Depot US$62m, as good a demonstration as any that money spent on security is a good investment. Such spectacular failures as these can do untold damage to a brand, leading to loss of respect, trust and trade. For example, the attack on Sony's PlayStation Network in 2011 compromised 77m user accounts, is thought to have cost the firm US$170m, and the subsequent revelations of lax security and poor system design caused major damage to the brand.

## From one Target, to the next

The theft of card details from Target led to a large number of them appearing for sale on the rescator.cc site, which security researcher Brian Krebs has traced to Ukraine. Stolen card details on the site can command

prices up to US$100 each and it has become one of the largest clearinghouse for such data, with many hundreds of thousands of cards sold in a single batch.

For a graphic indication of just how big a problem these lapses in security and mass theft of details have become, take a look at this beautiful and detailed interactive graphic at Information is Beautiful. While not as large as the loss suffered by Adobe last year (150m accounts), the attack on Home Depot could pose considerably greater danger of theft and fraud as it includes financial details and not just user accounts.

Once again, the extent to which people rely on terrible, easy-to-guess passwords is made very clear by the data stolen from Adobe and released to the web: the top five passwords of Adobe users were "123456", "123456789", "12345678", "password" and "adobe123". These are no more secure than no password at all – truly, for cybercriminals it is like shooting fish in a barrel.

So while defences have toughened up on the back-end, the risk now is at the front-end, which is exposed to a range of different web browsers, devices and environments. If each credit card is worth up to US$100, then there is ample incentive to find new and inventive ways of shooting these fish. For example, the malware used to attack Home Depot was completely new and unseen, showing that malware morphs and transforms to overcome defences against it. With the potential illicit profit to be made, the incentive is there for hackers to place considerable investment into creating a successful attack.

In barely 20 years we have created a complex and substantial e-commerce infrastructure from nothing. But we are failing to secure ourselves from large-scale fraud that will damage citizens, companies and economies. We need to invest in and design better ways of detecting,

protecting and analysing our electronic infrastructure and demand better implementations of them from those we do business with.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation