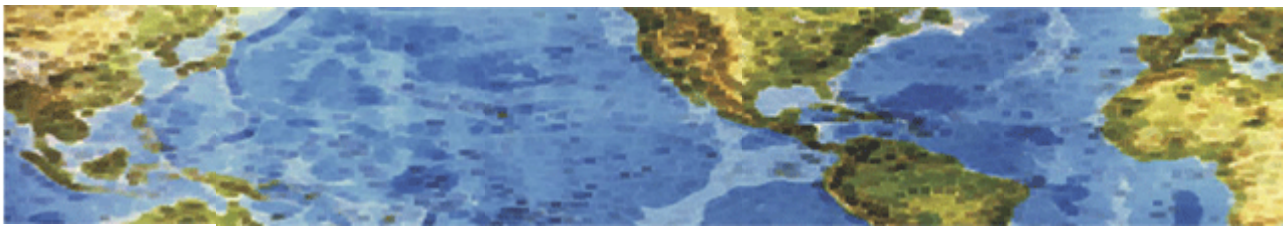
HALL ASSOCIATES



Risk-Based Decision Making Commentary
15 January 2014 Newsletter

Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen

Some additional information about the Target data breach covered in earlier newsletters –

Target disclosed that a data breach discovered last month exposed the names, mailing addresses, phone number and email addresses for up to 70 million individuals. "As part of Target's ongoing forensic investigation, it has been determined that certain guest information — separate from the payment card data previously disclosed — was taken during the data breach," the company said in a statement. "This theft is not a new breach, but was uncovered as part of the ongoing investigation. At this time, the investigation has determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals." Target said much of the data is partial in nature, but that in cases where Target has an email address, it will attempt to contact affected guests with informational tips to guard against consumer scams. The retail giant was quick to note that its email communications would not ask customers to provide any personal information as part of that communication. Watch out for email scams trying to get you to reveal even more personal information.

http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/

More well-known U.S. retailers victims of cyber attacks - sources

(Reuters) - Target Corp and Neiman Marcus are not the only U.S. retailers whose networks were breached over the holiday shopping season last year, according to sources familiar with attacks on other merchants that have yet to be publicly disclosed. Smaller breaches on at least three other well-known U.S. retailers took place and were conducted using similar techniques as the one on Target, according to the people familiar with the attacks. Those breaches have yet to come to light. Also, similar breaches may have occurred earlier last year.

The sources said that they involved retailers with outlets in malls, but declined to elaborate. They also said that while they suspect the perpetrators may be the same as those who launched the Target attack, they cannot be sure because they are still trying to find the culprits behind all of the security breaches. Law enforcement sources have said they suspect the ring leaders are from Eastern Europe, which is where most big cyber crime cases have been hatched over the past decade.

HALL ASSOCIATES

Only one well-known retailer, Neiman Marcus, has said that they too have been victim of a cyber attack since Target's December 19 disclosure that some 40 million payment card numbers had been stolen in a cyber attack. Neiman Marcus said it was not sure if the breach was related to the Target incident. Most states have laws that require companies to contact customers when certain personal information is compromised. In many cases the task of notification falls on the credit card issuer. Merchants are required to report breaches of personal information including social security numbers. It was not immediately clear if that was the case with the retailers who were attacked around the same time as Target.

SCRAPING MEMORY

Target has not disclosed how the attackers managed to breach its network or siphon off some of its most sensitive data. The sources who spoke to Reuters about the breaches said that investigators believe the attackers used similar techniques and pieces of malicious software to steal data from Target and other retailers. One of the pieces of malware they used was something known as a RAM scraper, or memory-parsing software, which enables cyber criminals to grab encrypted data by capturing it when it travels through the live memory of a computer, where it appears in plain text, the sources said. While the technology has been around for many years, its use has increased in recent years as retailers have improved their security, making it more difficult for hackers to obtain credit card data using other approaches.

Visa Inc issued two alerts last year about a surge in cyber attacks on retailers that specifically warned about the threat from memory parsing malware. The alerts, published in April and August, provided retailers with technical details on how the attacks were launched and advice on thwarting them. It was not clear whether Target's security team had implemented the measures that Visa had recommended to mitigate the risks of being attacked. Yet a law enforcement source familiar with the breach said that even if the retailer had implemented those steps, the efforts may not have succeeded in stopping the attack. That is because the attackers were more sophisticated than the ones in the previous attacks described in the Visa alerts, according to the source. The source asked not to be identified because they were not authorized to discuss the matter publicly.

DELAYED DISCLOSURE

Retailers are often reluctant to report breaches out of concern it could hurt their businesses. Target only acknowledged its 2013 attack after security blogger Brian Krebs reported the breach, prompting inquiries from journalists and investors. Neiman Marcus said an outside forensics firm discovered evidence on January 1 that indicated the retailer had been the victim of a cyber attack. It disclosed the breach nine days later, after another inquiry from Krebs, who was following up on reports about a surge in fraudulent charges traced to the retailer. Target and J.C. Penney Co Inc. waited more than two years to admit that they were victims in 2007 of notorious hacker Albert Gonzalez, who was accused of masterminding the theft and reselling of millions of credit cards and ATM numbers.

Investigators believe that the early series of attacks on retailers staged before late November were mostly used as trial attacks to help the hackers perfect new techniques they then used against Target, stealing payment cards at unprecedented speed.

http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112