KrebsonSecurity
In-depth security news and investigation

18 [illegible]

DEC 13

Nationwide retail giant **Target** is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a statement this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

Original story;

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

Minneapolis, Minn. based **Target Brands Inc.** has not responded to multiple requests for comment. Representatives from **MasterCard** and **Visa** also could not be immediately reached for comment.

Both sources said the breach was initially thought to have extended from just after Thanksgiving 2013 to Dec. 6. But over the past few days, investigators have unearthed evidence that the breach extended at least an additional week — possibly as far as Dec. 15. According to sources, the breach affected an unknown number of Target customers who shopped at the company's bricks-and-mortar stores during that timeframe.

"The breach window is definitely expanding," said one anti-fraud analyst at a top ten U.S. bank card issuer who asked to remain anonymous. "We can't say for sure that all stores were impacted, but we do see customers all over the U.S. that were victimized."

There are no indications at this time that the breach affected customers who shopped at Target's online stores. The type of data stolen — also known as "track data" — allows crooks to create counterfeit cards by encoding the information onto any card with a magnetic stripe. If the thieves also were able to intercept PIN data for debit transactions, they would theoretically be able to reproduce stolen debit cards and use them to withdraw cash from ATMs.

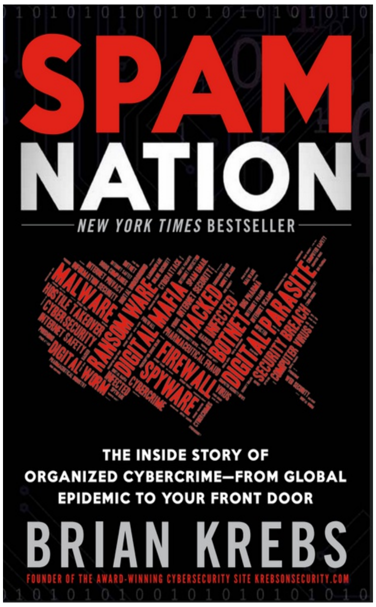
It's not clear how many cards thieves may have stolen in the breach. But the sources I spoke with from two major card issuers said they have so far been notified by one of the credit card associations regarding more than one million of cards total from both issuers that were thought to have been compromised in the breach. A third source at a data breach investigation firm said it appears that "when all is said and done, this one will put its mark up there with some of the largest retail breaches to date."

Some of the largest retailer breaches to date may help explain what happened in this case. In 2007, retailer TJX announced that its systems had been breached by hackers. The company later learned that thieves had used the store's wireless networks to access systems at its Massachusetts headquarters that were used to store data related to payment card, check and return transactions at stores across the country, and that crooks had made off with data from

[illegible]

Subscribe here

[illegible]


SPAM NATION
NEW YORK TIMES BESTSELLER
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

A New York Times Bestseller!

Buy at Amazon

Donate with PayPal

[illegible]

more than 45 million customer credit and debit cards.

In 2009, credit card processor Heartland Payment Systems disclosed that thieves had broken into is internal card processing network, and installed malicious software that allowed them to steal track data on more than 130 million cards.

This is likely to be a fast-moving story. Stay tuned for updates as they become available.

[EPSB]

[illegible]

Cards Stolen in Target Breach Flood Underground Markets" …Credit and debit card accounts stolen in a recent data breach at retail giant Target have been flooding underground black markets in recent weeks, selling in batches of one million cards and going for anywhere from $20 to more than $100 per card, KrebsOnSecurity has learned.

[/EPSB]

Tags: target black friday breach, target data breach

This entry was posted on Wednesday, December 18th, 2013 at 2:33 pm and is filed under Other. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

[illegible]

kspahn
December 20, 2013 at 3:47 pm

Does anyone know if the card number of a Target Red Card should be changed that is just withdrawing funds from a checking account? I imagine so huh? Unfortunately I cannot get thru to Target to do this and the only way is via phone…..

A. Nonny Mouse
December 21, 2013 at 6:02 pm

It'd be a good idea to get a new card. In the meantime, keep a close eye on your checking account. If necessary, you could close your checking account, and get a new one.

I would think it'll be easier to get through to Target by phone in a few days. I was able to use the automated system to request a new Target credit card today, though I had to call a few times before I was able to get a connection.

laura m.
December 24, 2013 at 10:12 am

Why the hell would you want a Target card or ever do biz w/them again?? Lawsuits are now being filed nationwide. If anyone has to do biz w/ Target, pay cash; never trust them again for security same with TJMaxx.

st
December 20, 2013 at 4:03 pm

Target is saying that only the customers "In-Store were affected but I made a purchase on December 2, 2013, through Targets ONLINE store, and my debit card was compromised. My Bank has confirmed that my card was compromised after making an ONLINE purchase @ Target. The "unauthorized access" impacted ONLINE customers as well.

Heron
December 21, 2013 at 11:48 am

Your card could've been compromised in a different breach, or intercepted online.

You shouldn't use a debit card to make online purchases. Use a credit card instead.

Domain Theft Strands Thousands of Web Sites

U.S. Arrests 13, Charges 36 in 'Infraud' Cybercrime Forum Bust

Would You Have Spotted This Skimmer?

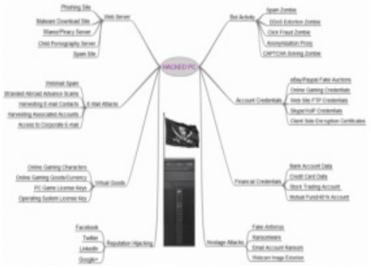
Alleged Spam Kingpin 'Severa' Extradited to US

Attackers Exploiting Unpatched Flaw in Flash

[illegible]

Click image for my skimmer series.

[illegible]



Badguy uses for your PC

[illegible]

Tools for a Safer PC

[illegible]