Maine Target shoppers' stolen card data for sale

The numbers are listed on a black market website run by a Russian hacker.

By J. Craig Anderson |December 21, 2013

Nearly 1,700 credit and debit card numbers stolen from shoppers at the five Target stores in Maine are for sale on at least one black market website, as thieves cash in on one of the largest data thefts in history.

The numbers stolen from Maine shoppers were among 1.5 million consumer accounts, all stolen from Target over a two-week period, that were available for prices ranging from about $20 to $100 each. The website, which allows buyers to search for account data according to such variables as issuing bank and the specific store from which the accounts were stolen, promised there would be more batches of card numbers for sale in coming days.

State officials previously could not confirm whether any Maine shoppers were affected by the massive Target data theft. They were shocked Friday when the Portland Press Herald showed them a black market site selling the card numbers.

"That's really unbelievable – an eBay-type shopping site for credit cards," said William Lund, superintendent of the Maine Bureau of Consumer Credit Protection.

So far, the black market site has listed for sale only a fraction of the estimated 40 million card numbers stolen from Target's U.S. stores between Nov. 27 and Dec. 15.

As of Friday, the website listed about 500 cards stolen from the Target store in South Portland, 450 from the Bangor store, 300 from the Topsham location, and more than 200 each from the Augusta and Biddeford stores.

Given that the credit and debit card numbers are actively being sold online, local cybersecurity experts urged Mainers who shopped at Target during the security breach to cancel the cards they used immediately.

"There are consumer protection laws against unauthorized charges, but it's easier just to call and cancel the cards and get new ones," said Joshua Silver, a shareholder in the Portland law firm Bernstein Shur and a cybersecurity specialist.

The black market website is being operated by a Russian hacker who goes by the name Rescator, and who is active on the digital underground forum Lampeduza, a gathering place for hackers and other cybercriminals, security analysts and bloggers said.

The Press Herald declined to publish the online address of the website because it is a criminal enterprise, and the danger to those who visit the site is unknown.

Card data have been added to the site in batches of about 120,000 to 500,000 at a time over the past 10 days. Any visitor to the site can register and browse the database.

Each listing shows the first six digits of the card number, also called the "bin number," which identifies the issuing bank. Also listed is the name of the bank, expiration date, whether it is a consumer, business, gold or platinum card, and the location from which the numbers were stolen. Location is important to thieves, since banks often flag a transaction as potentially fraudulent if it is made far away from where the card is customarily used.

The listing also indicates whether the data include detailed "Track 1" information, such as the cardholder's name and a security code embedded in the card's magnetic strip. The perpetrators of the Target heist did not obtain the three-digit security code imprinted on the back of most credit and debit cards, according to Target.

Finally, the website lists the asking price for each card's data, which in most cases is between $20 and $50. The online purchaser can buy multiple items at a time via a shopping-cart system similar to that of Amazon.com and other e-commerce websites.

In order to make a purchase, the buyer must first send money to Rescator and his accomplices, either via a virtual currency such as Bitcoin or a wire transfer to Western Union in Lviv, Ukraine.

"A lot of these schemes are run from Eastern Europe," Silver said. "It's a hacking mecca."

Neither the retailer nor law enforcement officials have disclosed how the thieves managed to steal millions of consumer payment card numbers.

Brian Leary, spokesman for the U.S. Secret Service, which investigates financial fraud, said he could not comment because the matter is still under investigation.

However, blogger and digital security expert Brian Krebs, who broke the Target heist story Wednesday, explained on the website krebsonsecurity.com that fraud investigators at a handful of unnamed banks first discovered that card information had been compromised after their customers shopped at Target. They informed Target officials, who then began their own investigation, according to Krebs.

Minneapolis-based Target Brands Inc. acknowledged Thursday that hackers had stolen information from as many as 40 million credit and debit cards that were used to make purchases at all of its stores in the U.S.

Card transactions at Target are now safe, the company said in a news release. Online transactions at Target.com were not affected, the company said.

Target representatives have not specified how many customers in Maine were affected, and did not return calls seeking comment.

Without more specific information, it is difficult to determine exactly how many Maine shoppers may have been affected.

However, based on the percentage of card data from Maine on the black market site, the total number of cards stolen from Mainers would total more than 45,000 if the hackers listed all 40 million stolen cards.

The card information would not be sufficient to make online purchases from most websites, because it does not include debit card Personal Identification Numbers – or PIN – or the three-digit code included on the back of most cards. Even without the three-digit code and PIN, criminals can use the card data to "clone" cards and use them to make in-store purchases.

The stolen data also don't include the cardholder's address, although that information would be easy enough to look up, said Edward Sihler, technical director of the Maine Cybersecurity Center at the University of Southern Maine.

"Google," he said, "is a wonderful thing."