The Target Breach:

How it happened and tips for staying safe

CSID.COM

CSID®

A part of Experian

THE BREACH

The security breach at Target has been the subject of intense scrutiny and speculation throughout 2014. From November 27 to December 15, 2013, cyber criminals stole millions of customer records after installing malware on Target's Point of Sale (POS) system. The breach, which was strategically timed for the busy holiday shopping season, resulted in approximately 40 million stolen customer debit and credit cards, including card expiration dates, security codes and PIN numbers. Personal information for more than 70 million customers was also stolen including names, mailing addresses, email addresses and phone numbers. The underlying cause of this enormous breach – someone clicked on a malware-ridden link in a phishing scam.

> **The underlying cause of this enormous breach – an employee from one of Target's third-party vendors clicked on a malware-ridden link in a phishing scam.**

There are different ways that POS malware can get into a system. In Target's case, cyber criminals used stolen credentials from a third party vendor to access Target's network. The cyber criminals then laterally gained access to other parts of the network until they were able to infect the company's POS system with malware.

THE RESPONSE

On January 13, 2014, Target confirmed that malware was found and removed from the company's POS devices. POS malware is designed to extract payment data from the computer terminals where purchases are made in a store. The malware identifies where payment information is stored on a POS system prior to being encrypted and processed. The malware then steals the sensitive data and copies it to an online server where cyber criminals can access whenever and wherever.

Since the breach, the CSID, a part of Experian, CyberAgent technology has found more than 152 million compromised credentials related to the Target breach. It has been estimated that the cost of this breach to banks, retailers and consumers could exceed $18 billion.

TIPS FOR STAYING SAFE

The FBI has since warned U.S. retailers and consumers to prepare for further cyber attacks on store POS systems, after linking malware used in the attack on Target to 20 other attacks in 2013. This type of malware is inexpensive and can be incredibly profitable for the cyber criminal.

The only way to completely avoid your credit and debit card information from being compromised on a POS system is to pay by cash – a solution that is not always convenient or possible.

Some more practical ways to prepare for the threat of POS malware include:

- Keep an eye on personal info with an identity protection service. The Target breach not only resulted in stolen credit and debit cards numbers but personal information as well – information that can be used for identity theft and other types of fraud. An identity protection service can alert you when your personal information has been compromised and is being used for nefarious purposes. Target has offered a free year of identity protection to its affected shoppers. To take advantage of this offer, visit creditmonitoring.target.com.

- Keep an eye on your credit and debit statements for odd charges. Keep an eye on all transactions – even small ones. Cyber criminals often test accounts with small transactions to make sure they are active. If you see suspicious transactions, report them as soon as possible and request a new card.

- Consider paying with credit cards when making in-store purchases. Credit card companies cannot hold you liable for fraudulent purchases made on your card. This makes it a lot easier and quicker to recoup losses from a fraudulent credit card charge than when using a debit card and recouping losses from your bank.