Target breach linked to global cybercrime, researchers say

January 17 2014

A couple of shoppers leave a Target store on a rainy afternoon in Alhambra, California on December 19, 2013

The massive data breach at US retailer Target is probably linked to a broader global network of cybercrime that may have affected other merchants, security researchers said.

US security firm iSight Partners concluded that the hackers who stole data on as many as 110 million Target customers comes from "a new

piece of malicious software," which "has potentially infected a large number of retail information systems," according to a statement Thursday from the company, which has been working with US authorities.

A separate report by the Israeli-based firm Seculert said an analysis of the malware showed the attack "had two stages, which is a well known attribute of an advanced threat."

The malware first infected Target's checkout counters to extract credit numbers and sensitive personal details, "then after staying undetected for six days, the malware started transmitting the stolen data to an external FTP server, using another infected machine within the Target network" Seculert said.

Seculert said the hackers used a virtual private server (VPS) located in Russia to download the stolen data and "continued to download the data over two weeks." But the firm found no evidence of a link to other retailers such as Neiman Marcus, which was also compromised.

Jim Walter of McAfee Labs said in a blog post that his firm has found "credible evidence to indicate that the malware used in the Target stores attack is related to existing malware kits sold in underground forums."

Walter said the malware is similar in function to and possibly derived from a bug known as "BlackPOS" which first was detected last year.

Meanwhile researchers from IntelCrawler, a Los-Angeles based cyber intelligence company, said in a statement the BlackPOS malware was created by a 17-year-old hacker and has been used to infect retail systems in Australia, Canada and the US.

"The first name of the malware was a lyric 'Kaptoxa,'" which means

potato in Russian slang, according to a statement from IntelCrawler.

The firm said the malware was sold more then 40 times to cybercriminals from Eastern Europe and other countries, including the operators of sites selling stolen credit card data.

The US Secret Service, which is leading the investigation, declined to comment on the latest developments.

Target meanwhile began notifying some of its customers that it was offering one year of free credit monitoring, to help customers guard against identity theft or unauthorized charges to their debit or credit cards.