6-Computerworld-Target breach

Target breach happened because of a basic network segmentation error

Hackers gained access to Target POS systems using login credentials belonging to an HVAC company

By Jaikumar Vijayan

Computerworld |

The massive data breach at Target last month may have resulted partly from the retailer's failure to properly segregate systems handling sensitive payment card data from the rest of its network.

Security blogger Brian Krebs, who was the first to report on the Target breach, yesterday reported that hackers broke into the retailer's network using login credentials stolen from a heating, ventilation and air conditioning company that does work for Target at a number of locations.

According to Krebs, sources close to the investigation said the attackers first gained access to Target's network on Nov. 15, 2013 with a username and password stolen from Fazio Mechanical Services, a Sharpsburg, Pa.-based company that specializes in providing refrigeration and HVAC systems for companies like Target.

Fazio apparently had access rights to Target's network for carrying out tasks like remotely monitoring energy consumption and temperatures at various stores.

The attackers leveraged the access provided by the Fazio credentials to move about undetected on Target's network and upload malware programs on the company's Point of Sale (POS) systems.

The hackers first tested the data-stealing malware on a small number of cash registers and then, after determining that the software worked,

uploaded it to a majority of Target's POS systems. Between Nov. 27 and Dec. 15, 2013, the attackers used the malware to steal data on about 40 million debit and credit cards.

U.S., Brazil and Russia.

Krebs quoted Fazio's president, Ross Fazio, as confirming that the U.S. Secret Service had visited his company in connection with the Target breach. The company offered no other details on its alleged role in the breach.

Fazio did not immediately respond to a Computerworld request for comment. On Wednesday afternoon, the company's site appeared to be offline, though it was not immediately clear whether that had anything to do with Krebs' report.

Ever since Target first disclosed the data breach in December, the company has portrayed itself as the victim of an especially sophisticated cyber heist. Indeed, in testimony before Congress this week, Target executives defended the company's security practices and maintained that the breach was hard to avoid because of its sophisticated nature. *[Diminish, Reinforce]*

But Krebs suggests that the cause was much more mundane and wholly preventable, said Jody Brazil, founder and CTO at security vendor FireMon. "There's nothing fancy about the breach," Brazil said *[Disappointment]*.

"Target chose to allow a third party access to its network," but failed to properly secure that access, Brazil said. *[Disappointment]*

Even if Target had a valid reason for giving Fazio access, the retailer should have segmented its network to ensure that Fazio and other third parties had no access to its payment systems. *[Disappointment]*

Several mature processes and practices currently exist for securing third-party access to enterprise networks, Brazil said. Even the Payment Card Industry Data Security Standard, which companies like Target are required

to follow, specifies network segmentation as a way to protect sensitive cardholder data.

It was Target's responsibility to ensure that those practices were followed, Brazil said. But the fact that attackers were apparently able to leverage their third-party access to reach Target's payment systems suggests those practices were improperly implemented — at best, he said. *[Disappointment]*

The only really sophisticated component of the attack appears to have been the malware used to intercept and steal payment card data from Target's POS systems. But the attackers would have been unable to install the malware if Target had employed proper network segmentation practices in the first place, Brazil said *[Disappointment]*.

Stephen Boyer, CTO and co-founder of BitSight, a company that specializes in third-party risk management, said the breach highlights the threat posed to companies by network-connected outsiders.

"In today's hyper-networked world, companies are working with more and more business partners with functions like payment collection and processing, manufacturing, IT, and human resources," Boyer said. "Hackers find the weakest point of entry to gain access to sensitive information, and often that point is within the victim's ecosystem."

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at @jaivijayan or subscribe to Jaikumar's RSS feed . His e-mail address is jvijayan@computerworld.com .