Target Hackers Broke in Via HVAC Company

February 6, 2014 Krebs on Security

http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

Target spokeswoman **Molly Snyder** said the company had no additional information to share, citing a "very active and ongoing investigation."

It's not immediately clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target's payment system network. But according to a cybersecurity expert at a large retailer who asked not to be named because he did not have permission to speak on the record, it is common for large retail operations to have a team that routinely monitors energy consumption and temperatures in stores to save on costs (particularly at night) and to alert store managers if temperatures in the stores fluctuate outside of an acceptable range that could prevent customers from shopping at the store.

"To support this solution, vendors need to be able to remote into the system in order to do maintenance (updates, patches, etc.) or to troubleshoot glitches and connectivity issues with the software," the source said. "This feeds into the topic of cost savings, with so many solutions in a given organization. And to save on head count, it is sometimes beneficial to allow a vendor to support versus train or hire extra people."

CASING THE JOINT

Investigators also shared additional details about the timeline of the breach and how the attackers moved stolen data off of Target's network.

Sources said that between Nov. 15 and Nov. 28 (Thanksgiving and the day before Black Friday), the attackers succeeded in uploading their card-stealing malicious software to a small number of cash registers within Target stores.

Those same sources said the attackers used this time to test that their point-of-sale malware was working as designed.

By the end of the month — just two days later — the intruders had pushed their malware to a majority of Target's point-of-sale devices, and were actively collecting card records from live customer transactions, investigators told this reporter. Target has said that the breach exposed approximately 40 million debit and credit card accounts between Nov. 27 and Dec. 15, 2013.

DATA DROPS

While some reports on the Target breach said the stolen card data was offloaded via FTP communications to a location in Russia, sources close to the case say much of the purloined financial information was transmitted to several "drop" locations.

These were essentially compromised computers in the United States and elsewhere that were used to house the stolen data and that could be safely accessed by the suspected perpetrators in Eastern Europe and Russia.

For example, card data stolen from Target's network was stashed on hacked computer servers belonging to a business in Miami, while another drop server resided in Brazil.

Investigators say the United States is currently requesting mutual legal assistance from Brazilian authorities to gain access to the Target data on the server there.

It remains unclear when the dust settles from this investigation whether Target will be liable for failing to adhere to payment card industry (PCI) security standards, violations that can come with hefty fines.

Avivah Litan, a fraud analyst with Gartner Inc., said that although the current PCI standard (PDF) does not require organizations to maintain separate networks for payment and non-payment operations (page 7), it does require merchants to incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties — including vendor access for support or maintenance (see section 8.3).

In any case, Litan estimates that *Target could be facing losses of up to $420 million as a result of this breach*, including reimbursement associated with banks recovering the costs of reissuing millions of cards; fines from the card brands for PCI non-compliance; and direct Target customer service costs, including legal fees and credit monitoring for tens of millions of customers impacted by the breach.

Litan notes these estimates do not take into account the amounts Target will spend in the short run implementing technology at their checkout counters to accept more secure chip-and-PIN credit and debit cards. In testimony before lawmakers on Capitol Hill yesterday, Target's

executive vice president and chief financial officer said upgrading the retailer's systems to handle chip-and-PIN could cost $100 million.

Target may be able to cover some of those costs through a mesh network of business insurance claims. According to a Jan. 19 story at businessinsurance.com, Target has at least $100 million of cyber insurance and $65 million of directors and officers liability coverage.

Update, Feb. 6, 3:33 p.m. ET: Fazio Mechanical Services just issued an official statement through a PR company, stating that its "data connection with Target was exclusively for electronic billing, contract submission and project management." Their entire statement is below:

Fazio Mechanical Services, Inc. places paramount importance on assuring the security of confidential customer data and information. While we cannot comment on the on-going federal investigation into the technical causes of the breach, we want to clarify important facts relating to this matter:

- Fazio Mechanical does not perform remote monitoring of or control of heating, cooling and refrigeration systems for Target.

- Our data connection with Target was exclusively for electronic billing, contract submission and project management, and Target is the only customer for whom we manage these processes on a remote basis. No other customers have been affected by the breach.

- Our IT system and security measures are in full compliance with industry practices.

Like Target, we are a victim of a sophisticated cyber attack operation. We are fully cooperating with the Secret Service and Target to identify the possible cause of the breach and to help create proactive initiatives that will further enhance the security of client/vendor connections making them less vulnerable to future breaches.