11-BGR-It turns out Target

The massive breach that occurred around Thanksgiving last year could have been prevented by Target's existing security personnel and advanced security software, an extensive investigative report from Bloomberg Businessweek reveals. But instead, Target did nothing, allowing hackers to steal over 40 million credit cards , as well as personal data for over 70 million customers . *[Disappointment]*

Six months before the data heist, Target spent $1.6 million on a sophisticated anti-malware system called FireEye that actually caught the hack and could have automatically eradicated the malware without any human interaction. *[Reinforce]* But that feature was turned off, as it's believed the newly purchased, and tested system, was still mistrusted by Target's security personnel. *[Disappointment]* "Typically, as a security team, you want to have that last decision point of 'what do I do,'" Bombardier Aerospace chief information security officer said about FireEye, a software the company has been using for more than a year.

The same security system is employed by the CIA, the Pentagon and other spy agencies around the world, and has an interesting way of catching malware attacks in real-time instead of reacting to known malware only, as antivirus programs do. The system creates a parallel computer network on virtual machines that capture any data that comes from the web to Target, while attackers actually believe they're inside their target – no pun intended.

Bloomberg Businessweek cover

Thus, the system captured the first malware code on November 30 and issued an alert that was ignored *[Disappointment]*. After using credentials from a HVAC company working for Target , hackers uploaded as many as five versions of the malware, which was disguised with a name related to a component in a data center management product – BladeLogic. FireEye

was able to catch each one of them and escalate the warning alerts. But Target did not react to any of these notifications *[Disappointment]*.

Even the Symantec Endpoint Protection antivirus program used by Target detected the malware around Thanksgiving issuing appropriate warnings, that were also ignored. In fact, it looks like "the malware utilized is absolutely unsophisticated and uninteresting," according to McAfee director of threat intelligence operations Jim Walter. *[Disappointment]*

The company also has a team of security experts in Bangalore, that continuously monitors Target's network. The team got the alert on November 30, and passed it on to the security team in Minneapolis. "And then… Nothing happened." *[Disappointment]*

Only on December 2 did the hackers start downloading the collected data to Russia through U.S. servers where they have temporarily gathered the data. From the 1797 U.S. Target stores, the hackers collected over 11GB of data. Federal law enforcement was able to actually get the data which was carelessly left on the hackers' U.S. temporary servers, and contacted Target about the breach on December 12.

It took three more days for Target to publicly acknowledge the hack. During a testimony before U.S. Congress, Target "has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that company investigators went back to figure out what happened," without mentioning that the store could have prevented everything had the warnings been acknowledged in the first days. *[Deny]*

How the hackers broke in graphic | Image credit: Bloomberg Businessweek

A manhunt for the people responsible for the hack has begun, with the main suspect being an Ukrainian 22-year old hacker that has been caught before stealing private data from a popular forum in his own country. The identity of the person has apparently confirmed by various sources, although there's no clear evidence pointing at him. Because the hackers left various traces in the malware that helped investigators discover his presumed identity, it is believed he was the ringleader of a band of hackers that performed the attack – he was the George Clooney that hired the other members of an

Ocean 11-like team, and who wrote the malware which the others then used to mine data from Target's servers. Other clues left by the hackers suggest they may have been behind at least six other data thefts over the last two years.

Meanwhile, credit and debit cards stolen in the heist have been selling on the black market , with Target customers who shopped during the period the retail store's network was hacked already suffering the consequences. *[Disappointment]*

Target was hit with over 90 lawsuits related to the massive data breach, and spent over $61 million as of February 1 responding to the attack. *[Legal Action]*

The entire story of how the whole Target data hack happened will appear in print on Friday in the new issue of Bloomberg Businessweek, and is available online.

Chris Smith started writing about gadgets as a hobby, and before he knew it he was sharing his views on tech stuff with readers around the world. Whenever he's not writing about gadgets he miserably fails to stay away from them, although he desperately tries. But that's not necessarily a bad thing.

Popular News