

Heartland Payment Systems Hit By Data Security Breach

The systems penetrated by a malicious keylogger could result in a data breach that rivals the parent company of TJ Maxx in 2007.

By Thomas Claburn, InformationWeek
Jan. 20, 2009

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=212901505>

Heartland Payment Systems, a leading payment processing company, reported on Tuesday that its systems had been compromised by malware in 2008.

The data breach could turn out to rival the massive breach reported by TJX in 2007, which affected as many as 94 million credit card accounts. Heartland handles 100 million transactions per month for more than 250,000 businesses. But the company isn't yet ready to disclose the number of credit card accounts affected.

"We found evidence of an intrusion last week and immediately notified federal law enforcement officials as well as the card brands," said Robert H.B. Baldwin Jr., Heartland's president and CFO, in a statement. "We understand that this incident may be the result of a widespread global cyberfraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."

Heartland was alerted to the breach by reports of suspicious transactions from Visa and MasterCard.

In a phone interview, Baldwin said that the bulk of the exposed data consisted of credit card numbers and expiration dates, and that a subset of the exposed data also included credit card names.

Baldwin said his company couldn't yet reveal an accurate number of exposed accounts. "There are some numbers flying around now that aren't based on any discussion that Heartland has had with anyone," he said. "They are speculation. ... We just discovered this last week. We have been working around the clock to get data out to the public because it's consequential and we think it's important to be transparent on this."

In its statement about the breach, Heartland said that no merchant data, cardholder Social Security numbers, unencrypted personal identification numbers (PIN), addresses, or telephone numbers were exposed.

Baldwin said his company wasn't yet ready to disclose the dates when its network was exposed. "We can say, however, that this is fully contained," he said. "That is both our view and the view of the forensic auditors we brought in to work on this issue."

Baldwin said that the breach was the result of keylogging malware, which covertly captures anything typed on an infected computer, such as user names and passwords.

"There were two elements to it, one of which was a keylogger that got through our firewall," he said. "Then subsequently it was able to propagate a sniffer onto some of the machines in our network. And those are what was actually grabbing the transactions as they floated over our network."

A sniffer is similar in concept to a keylogger, but rather than merely capturing keystrokes, a sniffer captures entire data packets on a network.

Asked whether the data was read remotely from a locally stored file or transmitted to an external site, Baldwin said, "We don't know in what way there was egress or to what extent," he said. "And that's one of the frustrating things about this. We know that a lot of transactions go across our network; we don't know the percentage of transactions that the sniffer was able to grab. And we don't know the percentage of those that the bad guys were able to access."

He added that while investigators considered the possibility that an insider might have been involved, there was no information that suggested any insider involvement.

While the company's Web site says the company handles more than 4 billion transactions per year, Baldwin said only about 1 billion of those were on the legacy Heartland network that was breached. The remaining 3 billion, the result of an acquisition the company made last May of the network services division of Alliance Data Systems, go over a separate network, which wasn't affected by the breach, he said.

He added that while the company handles roughly 100 million transactions per month, the number of unique credit card numbers processed is significantly less than that because some transactions represent the same credit card number being used at different merchants. While the actual total of affected accounts will depend on the number of months that Heartland's network was exposed, Baldwin said the company wasn't yet ready to disclose a specific estimate.

Baldwin said that in addition to an undisclosed system that's being implemented to shore up the Heartland network's defenses, his company is taking a variety of other steps to improve security.

He explained, "There are a host of things we didn't go into that we're implementing, some larger, some smaller, all of which are designed to say, 'OK, we had a commitment to high security. We were PCI compliant -- that was certified in April of last year. Yet we had this problem. Clearly we need to do more.' So our IT team is implementing as many additional precautions as it can as quickly as possible.

"We are really crushed by this," said Baldwin. "It's absolutely antithetical to everything Heartland stands for. We will therefore be redoubling our efforts to be the best processor out there. We obviously are pained by the inconvenience any consumers will have and look forward to coming out of this a stronger company."

If this data breach represents heartache for Heartland, security vendors see it as an opportunity to play doctor. "As the Heartland breach illustrates, you can be PCI compliant and still be breached," said Phil

<http://www.informationweek.com/shared/printableArticleSrc.jhtml;jsessionid=CFIPUJX>
Y ... 1/26/2009 Heartland Payment Systems Hit By Data Security Breach

Neray, VP of security strategy at database security company Guardium, in an e-mailed statement. "Good compliance doesn't mean good security."