Backoff: malicious computer software for PoS systems

SAN FRANCISCO, USA: The US Department of Homeland Security has warned businesses to watch for hackers targeting customer data with malicious computer code like that used against retail company Target.

Retailers have been warned about the Backoff malware threat that is targeting point of sale machines to harvest credit card numbers and passwords. Image: The Next Digit

A hacker software weapon dubbed Backoff is "compromising a significant number" of businesses large and small, according to an advisory put out by the US Computer Emergency Readiness Team (CERT).

CERT urged those administering point-of-sale systems to check whether Backoff is mining information from transactions and to report any cases to the Secret Service.

"The impact of a compromised PoS system can affect both the businesses and consumer by exposing customer data such as names, mailing addresses, credit/debit card numbers, phone numbers and e-mail addresses to criminal elements," CERT said in an advisory.

"These breaches can impact a business's brand and reputation, while consumers' information can be used to make fraudulent purchases or compromise bank accounts." the CERT advisory said.

Malware identified last year

Backoff was first identified in 2013 and has been cited as a culprit in a set of Secret Service investigations.

Hackers have evidently been cracking into systems used to remotely accessed business or store network and then installing malware to harvest credit card numbers, passwords or other valuable data used for purchases.

Remote access features have become increasingly common as businesses manage systems at diverse locations from central offices or workers linked to headquarters from home or the field.

According to CERT hackers have been using "brute force" attacks which typically involved computer programs battering accounts with relentless guesses about user names or passwords, .

An advisory on the CERT website outlines what business system operators should watch for and suggests ways to deal with Backoff.

US supermarket chain Albertsons, which has 1,060 stores in the United States, and its former owner SuperValu revealed last week that their computer systems were raided by hackers seeking credit card data. However it was not immediately clear if the data had been stolen.

The hackers attacked sometime between 22 June 22 at the earliest and ended the intrusion on 17 July at the latest.

Both said the intrusion was brought under control and that their customers can make credit and debit card purchases at the stores with no reason for concern.

The break-in is reminiscent of one suffered by retail chain Target, which revealed last year that 40m bank accounts or credit cards had been compromised when its computer system was hacked between 27 November and 15 December last year.

Source: AFP via I-Net Bridge