# India is on radar of hackers stealing card details from ATM machines

2 min read . Updated: 31 Oct 2019, 03:02 PM IST

Abhijit Ahaskar

While the US and UK accounted for two-thirds of it of attacks, a new report by Group IB suggest that Indian users are among the most affected

The report claims that 98% of the details belong to Indian banks and more than 18% of the 5.5 lakh cards they analyzed belonged to a single Indian bank they did not name

**Topics**

ATMs | Hackers

Stolen credit and debit card details are among the top items on sale on the Dark Web (part of the internet that is not indexed). Cybersecurity firm Sixgil puts the number of credit and debit cards stashed on underground forums at over 23 million in the first half of 2019.

While the US and UK accounted for two-thirds of it, a new report by Group IB suggest that Indian users are among the most affected. Researchers at Group IB have discovered one of the largest card dumps with more than 1.3 million card details available at $100 per card on Joker's Stash, an online store on Dark Web that deals in stolen card details.

The report claims that 98% of the details belong to Indian banks and more than 18% of the 5.5 lakh cards they analyzed belonged to a single Indian bank they did not name.

Group IB could not figure out the source of the breach at the time the report was published, but they believe hackers acquired the card details through skimming devices, which were secretly planted on ATMs or PoS systems, because the data in the dump is mostly track 2 data, which includes information found on card's magnetic strip.

Attempts to steal card details from ATMs in India have increased in recent years. In 2018, Kaspersky detected a banking malware ATMDtrack, which was being used to target Indian banks.

Researchers at Kaspersky found the malware was planted on the ATMs to capture card details when the user slides them into the machine. Kaspersky believes ATMDtrack to be the handiwork of North Korea-backed Lazarus group, which attacked Sony Pictures in 2014, stole $81 million from a Bangladeshi bank in 2016, and is also linked to WannaCry attack of 2017.

Further research by Kaspersky revealed 180 new malware samples with similar code sequence similarities as ATMDtrack, but were used to target and spy on other devices. According to an October report, DTrack is believed to have been used to target a PC that was connected to the network used by NPCIL (Nuclear Power Corporation of India) in September.

In August 2018, ATM servers of an Indian cooperative bank Cosmos was targeted by a malware attack, enabling hackers to simultaneously withdraw a total of $13.5 million from multiple ATM machines.

According to Positive Technologies, most of the ATMs are not properly protected against network attacks. Their hard drives are also not encrypted, which makes it easier for hackers to install malware and take control over cash dispenser.

According to Kaspersky, the PC part of ATMs are easily accessible compared to cash deposit and dispenser in the machine.

ATMs running on older operating systems which are no longer supported by the software provider also increases the risk of zero day attacks as they are unlikely to receive patches. For instance, even after Microsoft decided to stop support for Windows XP, millions of ATMs in India were still running on the older OS.

According to experts, card details sold on Dark Web are typically used to create a fake copy of the original card and withdraw large amounts from ATMs.

## Topics

ATMs | Hackers