TLP AMBER: BANK ISLAMI - SYED

Date:
30.10.2018

Summary

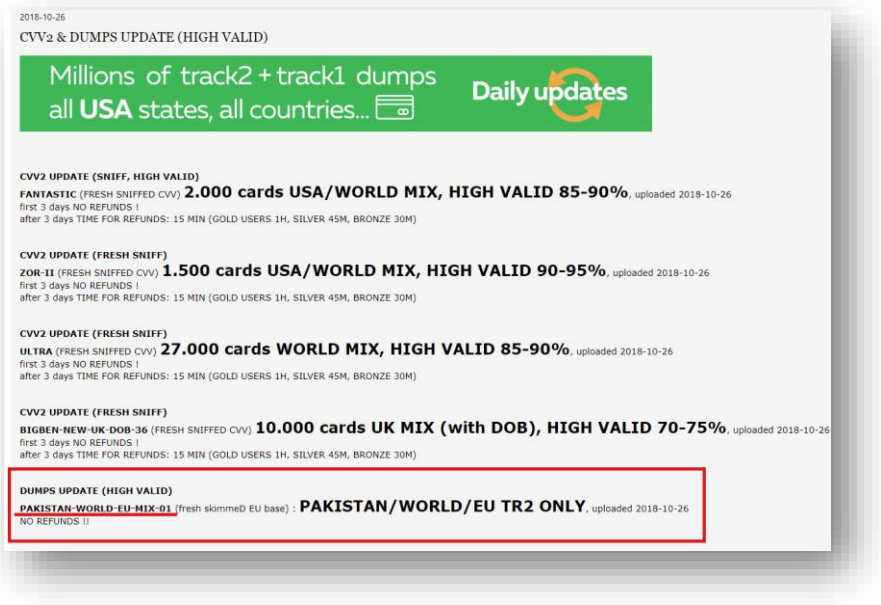
Category	Targeted attacks
Brief description	On 28.10.2018 Pakistan bank Bank Islami issued press release that they became victim of cybercrime attack. According to them, on the morning 27.10.2018 they detected abnormal transactions on one of its international payment card scheme. During these transactions a cybercrime group cashed out $2,6 million. On 26.10.2018 new dump under name "PAKISTAN-WORLD-EU-MIX-01" (10467 records) went on sale on cardshop Jokerstash. Analysis of previous incidents suggests that it is linked to the breach.
Threat	Jokerstash
Source geography	Pakistan
Source motivation	Financial
Admiralty code	B2 (Reliable/Probably True)
Target geography	Pakistan
Target industry	Financial Services
Risk	Compromise of data, moneythefts

Description

On 28.10.2018 Pakistan bank BankIslami issued a press release that they detected on the morning 27.10.2018 abnormal transactions on one of its international payment card schemes. Bank clients started to receive messages that somebody was cashing out money from their cards in different countries. During these transactions the attackers cashed out $2.6 million. From brief analysis and reference BankIslami appears to assume that it was cyber attack in which the network of the international payment scheme as well as that of the acquiring banks were possible compromised. This requires further incident response to confirm.

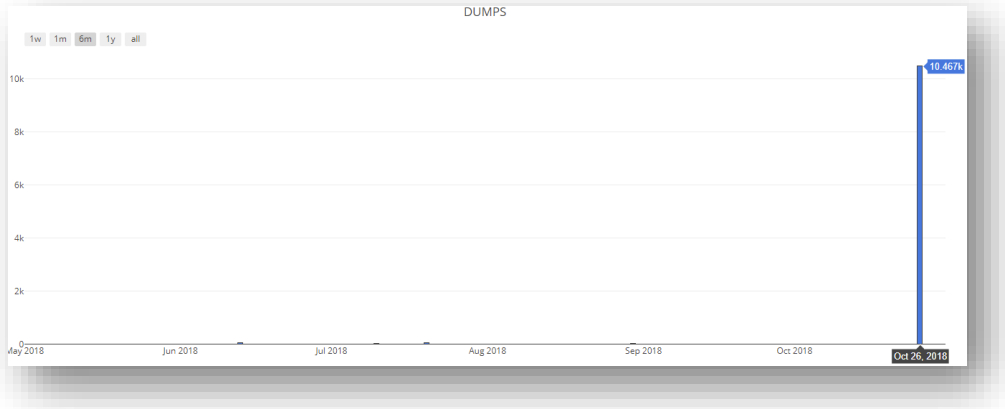
According to State Bank of Pakistan compromised cards were cash out via ATM and POS in different countries (they noted USA and Russia). At present they blocked all overseas transactions.

During cardshop monitoring we detected, that on 26.10.2018 new dump under name "PAKISTAN-WORLD-EU-MIX-01" went on sale on cardshop Jokerstash.



Picture 1 – Advertisement for new Pakistan base on cardshop

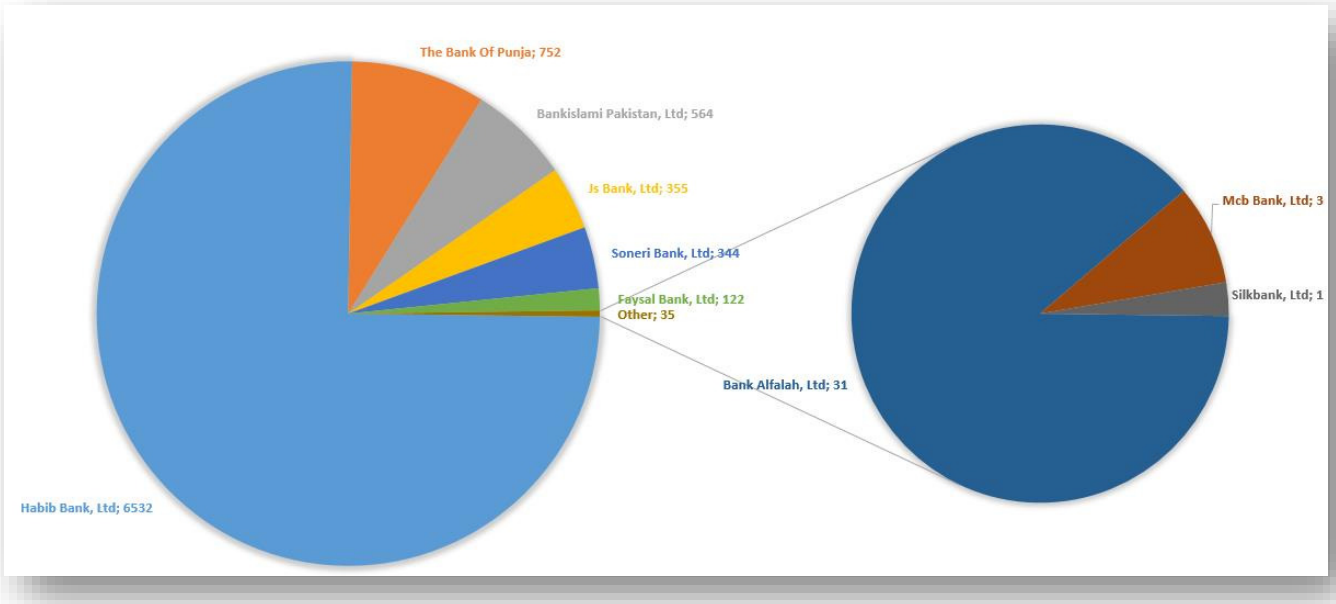
An interesting fact is that cards from this region are very rare on the cardshops, in the past six months it is the only one big sale of Pakistan cards.



Picture 2 – Graph of publication of cards belonged to Pakistan's bank

This base has 10467 dumps, 8704 belong to Pakistan's banks (including Bankislami):

- Habib Bank, Ltd.
- Js Bank, Ltd.
- Faysal Bank, Ltd.
- Soneri Bank, Ltd.
- Bankislami Pakistan, Ltd.
- The Bank Of Punjab
- Bank Alfalah, Ltd.
- Silkbank, Ltd.
- Mcb Bank, Ltd.



Picture 3 – diagram of cards from Pakistan's cards base

Beside these cards, there were 849 which belonged to banks from other countries and 914 dumps of undefined banks.

According to the name of this base on the cardshop, it is only first part of data which was uploaded to Jokerstash. Taking into account the facts that this base appeared on the cardshop right before detection of fraud activity in transactions of Bankislami bank and that it is the only big case involving Pakistani cards, most likely this sale is related to mentioned cybercrime attack.

It is probable that the cards were compromised before 26.10.2018, and then part of them were used by the cybercrime group to cash out via the international payments network and other cards were sold to Jokerstash cardshop.