PakCERT Threat Intelligence Report PCTI-2018-0111

Analysis of the recent attack on Pakistani banks

By Qazi Mohammad Misbahuddin Ahmed, CISSP, CPTS, CEH, ITIL, COBIT, MBCI
QA@PAKCERT.COM

4th November, 2018

Background

During mid October, customers who subscribed to banking transaction notifications started receiving alerts of money transfer from their accounts. BankIslami noticed abnormal transactions of Rs.2.6 million on the morning of 27th October and shutdown its international payment scheme.

Subsequently several others bank issued security alerts and either completely blocked customer's debit and credit cards or blocked their online and international use. Customers were sent SMS notifications of the changes.

The Attack

On 26th October 2018, a data dump was posted on Darkweb with over 9,000 debit cards, most of which belonged to customers of Pakistani banks. Even though BankIslami came in the limelight and initially the media reported the breach of a single bank but the dump showed a different story as it contained thousands of debit cards of several other banks in Pakistan.

BIN	Credit/?	Level	TR1+2/TR2	Issuer	Country	SCode	Price
536619	Debit	Standard	TR2	Habib Bank, Ltd	Pakistan		$100
462883	Debit	Gold	TR2	Bankislami Pakistan, Ltd	Pakistan		$135
437460	Debit	Gold	TR2	Js Bank, Ltd	Pakistan		$125
490471	Debit	Classic	TR2	Habib Bank, Ltd	Pakistan		$100
421500	Debit	Classic	TR2	Standard Chartered Bank	Pakistan		$100
536619	Debit	Standard	TR2	Habib Bank, Ltd	Pakistan		$100
538967	Debit	Prepaid	TR2	The Bank of Pubjab	Pakistan		$110
454535	Debit	Platinum	TR2	Faysal Bank, Ltd	Pakistan		$125
454526	Debit	Classic	TR2	Bank Alfalah, Ltd	Pakistan		$100

Screenshot of first dump from Darknet

Details of 8864 debit cards were inside the Darknet dump belonging to customers from the following 9 Pakistani banks:

No.	Bank Name	Type of Cards in the Darknet Dump	Number of Cards
1.	Bank Alfalah, Ltd	VISA (Prepaid, Classic, Platinum)	28
2.	BankIslami Pakistan, Ltd	VISA (Classic, Gold)	508
3.	Faysal Bank, Ltd	VISA (Classic, Gold, Platinum)	120
4.	Habib Bank, Ltd	VISA (Classic) Mastercard (Standard, Titanium, World)	6170

5.	Js Bank, Ltd	VISA (Classic, Gold)	355
6.	Samba Bank	Mastercard (Standard)	16
7.	Soneri Bank, Ltd	Mastercard (Standard, Gold)	333
8.	Standard Chartered Bank	VISA (Classic)	586
9.	The Bank of Punjab	Mastercard (Prepaid, Standard, Gold, Platinum)	748
		TOTAL	**8864**

The compromised cards were being sold at the following price:

No.	Bank Name	Bank Identification Number (BIN)	Darknet Price
1.	Bank Alfalah, Ltd	486248 (VISA Prepaid) 402581 (VISA Classic) 422070 (VISA Platinum)	$110 $100 $125
2.	BankIslami Pakistan, Ltd	462882 (VISA Classic) 462883 (VISA Gold)	$110 $135
3.	Faysal Bank, Ltd	454526 (VISA Classic) 454528 (VISA Gold) 454535 (VISA Platinum) 427297 (VISA Platinum)	$100 $125 $125 $125
4.	Habib Bank, Ltd	536619 (Mastercard Standard) 536632 (Mastercard Titanium) 517420 (Mastercard World) 490471 (VISA Classic)	$100 $125 $150 $100
5.	Js Bank, Ltd	437459 (VISA Classic) 437460 (VISA Gold)	$100 $125
6.	Samba Bank	534564 (Mastercard Standard)	$100
7.	Soneri Bank, Ltd	537939 (Mastercard Standard) 532126 (Mastercard Gold) 529779 (Mastercard Gold)	$100 $125 $125
8.	Standard Chartered Bank	421500 (VISA Classic)	$100
9.	The Bank of Punjab	538967 (Mastercard Prepaid) 536072 (Mastercard Standard) 529729 (Mastercard Gold) 515724 (Mastercard Platinum)	$110 $110 $135 $125

Just when everyone thought the storm is over, on 31st October 2018, a second dump of over 12 thousand cards was posted on Darknet comprising of 11000 cards from Pakistani banks.

BIN	Credit/?	Level	TR1+2/TR2	Issuer	Country	SCode	Price
464578	Debit	Platinum	TR1+2	Standard Chartered Bank	Pakistan		$135
428273	Debit	Classic	TR1+2	Dubai Islamic Bank	Pakistan		$110
524521	Debit	Titanium	TR1+2	Meezan Bank, Ltd	Pakistan		$125
450086	Debit	Gold	TR1+2	United Bank, Ltd	Pakistan		$135
420251	Debit	Signature	TR1+2	Bank Alfalah, Ltd	Pakistan		$160
536619	Debit	Standard	TR1+2	Habib Bank, Ltd	Pakistan		$100
428667	Debit	Classic	TR1+2	MCB Bank, Ltd	Pakistan		$100
476215	Debit	Classic	TR1+2	Allied Bank, Ltd	Pakistan		$110
517420	Debit	World	TR1+2	Habib Bank, Ltd	Pakistan		$150

Screenshot of second dump from Darknet

Details of 11000 debit cards were inside the second Darknet dump belonging to customers from the following 21 Pakistani banks:

No.	Bank Name	Type of Cards in the Darknet Dump	Number of Cards
1.	Al Baraka Bank Pakistan	Mastercard (Standard, Gold)	25
2.	Allied Bank, Ltd	VISA (Classic) Mastercard	741
3.	Askari Bank, Ltd	VISA (Classic, Gold) Mastercard (Gold)	493
4.	Bank Alfalah, Ltd	VISA (Prepaid, Classic, Gold, Platinum, Signature)	795
5.	Bank Al Habib, Ltd	VISA (Classic, Gold)	489
6.	Dubai Islamic Bank	VISA (Classic, Platinum)	199
7.	Faysal Bank, Ltd	VISA (Prepaid, Classic, Gold, Platinum, Signature)	458
8.	Habib Bank, Ltd	VISA (Classic) Mastercard (Standard, Titanium, World)	2043
9.	Habib Metropolitan Bank	VISA (Classic, Gold, Platinum)	344
10.	Js Bank, Ltd	VISA (Classic, Gold)	163
11.	Kasb Bank, Ltd	VISA (Prepaid)	2
12.	MCB Bank, Ltd	VISA (Prepaid, Classic, Gold, Platinum)	1125
13.	Meezan Bank, Ltd	VISA (Classic, Gold, Platinum	1375

		Mastercard (Standard, Platinum, Titanium)	
14.	NiB Bank, Ltd	Mastercard (Standard)	8
15.	Samba Bank	Mastercard (Standard)	14
16.	Silkbank, Ltd	VISA (Classic)	146
17.	Standard Chartered Bank	VISA (Classic, Platinum) Mastercard (Standard)	733
18.	Soneri Bank, Ltd	VISA (Classic, Gold) Mastercard (Standard, Gold)	162
19	Summit Bank, Ltd	VISA (Classic, Gold)	184
20.	The Bank of Punjab	Mastercard (Prepaid, Standard, Gold, Platinum)	120
21.	United Bank Limited	VISA (Prepaid, Classic, Gold) Mastercard (Standard, Platinum)	1381
		TOTAL	**11000**

No card details from BankIslami were in the second dump but several more banks were found.

The compromised cards from the second dump were being sold at the following price:

No.	Bank Name	Bank Identification Number (BIN)	Darknet Price
1.	Al Baraka Bank Pakistan	540345 (Mastercard Standard) 537975 (Mastercard Standard) 519828 (Mastercard Gold) 539136 (Mastercard Gold)	$110 $110 $135 $135
2.	Allied Bank, Ltd	476215 (VISA Classic) 220544 (Mastercard)	$110 $125
3.	Askari Bank, Ltd	479765 (VISA Classic) 479766 (VISA Gold) 514010 (Mastercard Gold)	$110 $135 $125
4.	Bank Alfalah, Ltd	486248 (VISA Prepaid) 402581 (VISA Classic) 402583 (VISA Classic) 486247 (VISA Classic) 421339 (VISA Gold) 466062 (VISA Gold) 461758 (VISA Platinum) 422070 (VISA Platinum)	$110 $110 $110 $110 $135 $135 $135 $125

		420251 (VISA Signature)	$160
5.	Bank Al Habib, Ltd	437584 (VISA Classic) 437585 (VISA Gold)	$110 $135
6.	Dubai Islamic Bank	428273 (VISA Classic) 483565 (VISA Classic) 441574 (VISA Platinum)	$110 $135 $135
7.	Faysal Bank, Ltd	490245 (VISA Classic) 428325 (VISA Classic) 454526 (VISA Classic) 458866 (VISA Classic) 454528 (VISA Gold) 428344 (VISA Gold) 454535 (VISA Platinum) 427297 (VISA Platinum) 472468 (VISA Platinum) 434993 (VISA Signature)	$110 $110 $110 $110 $125 $135 $125 $125 $135 $160
8.	Habib Bank, Ltd	403528 (VISA Classic) 490286 (VISA Classic) 490471 (VISA Classic) 421485 (VISA Classic) 536619 (Mastercard Standard) 536632 (Mastercard Titanium) 517420 (Mastercard World)	$100 $100 $100 $100 $100 $125 $150
9.	Habib Metropolitan Bank	437452 (VISA Classic) 437453 (VISA Gold) 437455 (VISA Platinum)	$100 $125 $125
10.	Js Bank, Ltd	437459 (VISA Classic) 437460 (VISA Gold)	$100 $125
11.	Kasb Bank, Ltd	458481 (VISA Prepaid)	$110
12.	MCB Bank, Ltd	436532 (VISA Prepaid) 428667 (VISA Classic) 420262 (VISA Gold) 428668 (VISA Gold) 428669 (VISA Platinum)	$110 $100 $125 $125 $125
13.	Meezan Bank, Ltd	464951 (VISA Classic) 464952 (VISA Gold) 437525 (VISA Platinum) 516067 (Mastercard Standard)	$110 $135 $135 $100

		538086 (Mastercard Platinum) 524521 (Mastercard Titanium)	$125 $125
14.	NiB Bank, Ltd	546369 (Mastercard Standard)	$100
15.	Samba Bank	534564 (Mastercard Standard)	$100
16.	Silkbank, Ltd	484838 (VISA Classic) 484871 (VISA Classic)	$110 $110
17.	Standard Chartered Bank	421310 (VISA Classic) 421500 (VISA Classic) 462886 (VISA Classic) 421501 (VISA Platinum) 464578 (VISA Platinum) 407569 (VISA Platinum) 545249 (Mastercard Standard)	$110 $100 $110 $135 $135 $125 $100
18.	Soneri Bank, Ltd	461688 (VISA Classic) 461689 (VISA Gold) 537939 (Mastercard Standard) 532126 (Mastercard Gold) 529779 (Mastercard Gold)	$110 $135 $100 $125 $125
19	Summit Bank, Ltd	458539 (VISA Classic) 458540 (VISA Gold)	$110 $135
20.	The Bank of Punjab	538967 (Mastercard Prepaid) 536072 (Mastercard Standard) 529729 (Mastercard Gold) 515724 (Mastercard Platinum) 526922 (Mastercard Platinum)	$110 $110 $135 $125 $125
21.	United Bank Limited	437743 (VISA Prepaid) 421461 (VISA Classic) 450084 (VISA Classic) 421462 (VISA Gold) 450086 (VISA Gold) 540375 (Mastercard Standard) 532709 (Mastercard Platinum)	$110 $110 $110 $135 $135 $110 $135

What exactly happened?

Hacked credit card data is available in 2 formats on Darknet. Text based credit card details like Full Name, Address, Phone number, Card Number, Expiry and CVV2 which can be easily used by someone for illegal online purchases. The second format is skimmed dumps which means the hacker was physically

able to scan the card details possibly at a compromised ATM or merchant machine. These skimmed card details are used to create a duplicate card which can then be used at an ATM or merchant machine for illegal transactions.

A total of 19,864 cards were compromised from 22 Pakistani banks. This number does not include a small number of other compromised cards which were found in the dumps.

These belong to banks outside Pakistan like National Bank of Abu Dhabi, Abu Dhabi Islamic Bank, Emirates Nbd, Commonwealth Bank of Australia, Citibank USA, etc. which shows that it includes data from visitors who traveled to Pakistan during this time and used one of the compromised ATM or merchant machine.

Initially there were rumours of BankIslami servers being hacked but looking at the number of total compromised cards and that too belonging to 22 different banks, it is evident that several compromised ATMs or merchant machines were involved in the skimming.

Platinum, Business and World Elite cards from Citibank (USA) with very high transaction limits are sold costing between $1 to $35 on Darknet. The transaction limit on an average Pakistani card is much less so it is surprising to see the prices of $100 - $160 for these cards. Why would an attacker buy such expensive cards when they can buy cheaper cards with much higher transaction limit? This question leads to two possibilities:

1. The people who initially did the skimming were visitors from outside Pakistan. They used the cards themselves and then put the dumps for sale on Darkweb.

2. The people who skimmed were locals and helped a more advance group outside Pakistan. The locals had the dumps and so decided to put it on Darkweb with a higher price in order to make some quick profit.

A detailed investigation will surely help in identifying and catching the culprits. Meanwhile our banks need to do a root cause analysis to Identify and plug the gaps to improve security. Subscription to threat intelligence service from the information security industry should be a top priority as the first dump was posted a day before the incident and the second dump is already here.

This report will be updated as we gather more information.

Statistics about the compromised cards in both dumps will be made available on our website at http://www.pakcert.com/

PakCERT (Pakistan Computer Emergency Response Team)
Suite 503, 5th Floor, Sky Mark Tower, Block 7/8, K.C.H.S. Shahrah-e-Faisal Karachi – Pakistan
(0092) 0302-2442999
(0092) 0300-9253092