IIMC-CRC-2014-06

IIMC CASE RESEARCH CENTRE (IIMCCRC)
PRIYA SEETHARAMAN, SAIKAT LAHIRI
MARCH 2014

BANK OF DASTAAN: UNLIMITED OPERATIONS CYBERATTACK

FEBRUARY 18, 2013 10:30 PM, DASTAAN

Yakub was bored. As he watched the 6 screens flashing in front of him, he said a quiet prayer that a year from now he would be doing something else. His job as a cybersecurity contractor at the Bank of Dastaan (BoD) in one of the major financial hubs of the Middle East may have sounded exciting to outsiders, but it turned out to be a lot of watching screens and monitoring alerts for 8-hour shifts every day. Anybody could have done this; his skills as a cybersecurity expert and a certified ethical hacker had not been called into play even once during his one-month stint here. All that was about to change in the next few hours.

He made himself some coffee and walked back to his desk, waving hello to his colleague Ahmad who sat across the room from him. As he settled back in, something on one of the monitors caught his attention. There was a little red dot on the screen. It indicated that someone had just tried to use a "flagged"[1] plastic card issued[2] by the BoD. It was at an ATM in New York City, near Times Square in the heart of Manhattan. His coffee forgotten, he keyed in some commands rapidly and realized that the card had been flagged as one of those used in a cyberattack on BoD and two other banks a couple of months back. Yakub and some others, including Ahmad, had been hired right after that attack as part of the bank's measures to strengthen its cybersecurity.

---

[1] A card that has been used illegally is often "flagged" in order to prevent and detect attempts to use in the future.

[2] A credit or debit card is issued by an organization, often a financial services provider, such as a bank. "Issuer" is a term used to refer to the organization that provides the credit or debit card to the customer. The issuer bears the risk, essentially vouching for the creditworthiness of the customer.

Of course, this attempt using the same card had failed, but it had raised a trigger for Yakub sitting thousands of miles away. Suddenly on full alert, Yakub put on his headset and pondered what to do. Should he try to handle this himself or should he escalate the problem right away? Maybe he could ask Ahmad to lend him a hand. After a minute or two of indecision, he finally decided to call his boss, Darren, a 20-year veteran of the cybersecurity business and head of information security for the bank. Darren was known to have been a technology wizard in his younger days and had spent a lot of his working life as an information security programmer in the west.

"This is Darren," said the familiar voice at the other end.

"Darren, Yakub here. Sorry to bother you so late at home. Do you have a minute?"

"Of course. What's up?"

Yakub explained briefly. When he was finished, Darren said, "I cannot believe this could be happening again."

He paused for a few seconds, thinking.

"Yakub, home in on that ATM right now. Check every transaction that happened on it in the last few minutes before and after the failure."

Yakub typed rapidly and within a few seconds the transactions were on his screen. He whistled softly.

"What's going on Yakub?" Darren sounded calm.

"Darren, the next 5 transactions happened within 5 minutes of the failure, each for USD 4,000, with a different card. All were with our cards."

"What type of cards?"

"Prepaid debit cards.[3] All of them."

"Four grand on prepaid cards!" Darren was not calm any more. "Check the limits[4] on those cards right now."

A few keystrokes later Yakub spoke again "Each of them has a limit of USD 100,000." He suddenly thought of something and said, "Hang on a second here, Darren." Some more rapid typing, some clicking of the mouse and Yakub gave out a little exclamation.

"Darren, you will not believe this. The same five cards again, at a different ATM, in Queens, New York. This time USD 5,000 each."

"Ok, who has a USD 100,000 limit on a prepaid card? And only Superman can go from Times Square to Queens in less than 5 minutes. My guess is this guy is not Superman."

---

[3] Prepaid debit cards act much like regular debit cards; the value associated with the card is stored in the customer's account with the issuer.

[4] A "limit" or "credit limit" is the maximum amount that the customer is permitted to spend on a credit or debit card. The user's credit worthiness in case of credit cards and their usable account balance in case of debit cards usually determine this limit.

"What do you want to do, Darren?"
"This is way above my pay grade, Yakub. After all, I am a contractor as well. Keep tracking those cards. I am going to conference Srinath. Hold on."
Srinath was the Chief Operating Officer and General Manager, effectively the second in command after the CEO.[5] Darren reported to him. In two minutes, Srinath was on the line and apprised of the situation.
"Again! How is this possible, Darren? When we met in January to discuss this[6], you said it was a one-in-a-million chance the first time. We even hired the four new contractors for monitoring our systems as you recommended. Should we have done something more?"
"Srinath, all our firewalls and patches are in place and up to date, I'm sure. What can we do if lightning strikes twice in the same place? And good for us we hired those four guys. Yakub here is the one who detected what was happening."
"All right, Darren. I am going to call the police right away. They will definitely want to speak to you to get more details. I will give them your number."
"Sure Srinath, whatever you need."
"I will speak to the CFO and our legal team as well and let them know what's coming. We have to make sure our customers do not panic. I cannot bother Mahmoud [the CEO] at this late hour. I will call him in the morning and decide what we should tell our clients. Anyway, don't worry about that now; you keep doing your thing, Darren. I'll be in touch."

[5] See **Exhibit 1** for a partial organization chart.

[6] See **Exhibit 2** for excerpts from minutes of the meeting held on January 2, 2013.