

North Korean Hacking Group Steals \$13.5 Million From Indian Bank

DR darkreading.com/attacks-breaches/north-korean-hacking-group-steals-135-million-from-indian-bank-/d/d-id/1332678

Jai Vijayan

August 27, 2018



Attacks/Breaches

5 MIN READ

ARTICLE

Tactics that Lazarus Group used to siphon money from India's Cosmos Bank were highly sophisticated, Securonix says.

August 27, 2018

North Korean-linked Lazarus Group is believed responsible for stealing \$13.5 million from India's Cosmos Bank in a brazen attack that has exposed limitations in the measures banks use to defend against targeted cyber threats.

The theft occurred between August 10 and August 13, 2018, and was enabled via thousands of fraudulent ATM transactions across 28 countries and by at least three unauthorized money transfers using the bank's access to the SWIFT international financial network.

It is still unclear how the threat actors managed to initially infiltrate the bank's network. But based on how Lazarus Group actors have typically operated in the past, the attackers broke in via a spear-phishing email and then moved laterally within the bank's network, according to researchers at Securonix.

"This attack is a good example of the fact that, while ATM and SWIFT transaction monitoring is important, it often is not enough, and may only give you 10%-20% of the required detection coverage," the security vendor noted in its report.

The Cosmos Co-operative Bank is a 111-year old co-operative bank in India with branches in 7 states and 39 major cities. Between August 10 and August 11, Lazarus Group operators managed to compromise an end-user system at the bank and used that to access and compromise the institution's ATM infrastructure.

Publicly available information and Securonix' own analysis suggest that the attackers used multiple targeted malware exploits to set up a malicious ATM/POS proxy switch in parallel with Cosmos Bank's own central switch.

They then broke or redirected the connection between the bank's ATM/POS central switch and its back-end Core Banking System. Securonix described the banking switch as a component that is primarily used to perform routing and transaction-processing decisions.

"Based on the publicly available details, most likely there was no additional hardware installed," says Oleg Kolesnikov, a member of the Securonix threat research team. "The malicious payment switch typically comes in the form of software, so this is likely what was installed and/or cloned/modified by the attackers to proxy the requests from the ATM terminals instead of the existing switch."

ATM Withdrawals

The attackers are believed to have increased the withdrawal limits on hundreds of targeted accounts at the bank and set them up so cash withdrawals could be made from the accounts from abroad. In total, operators working on behalf of Lazarus Group used 450 cloned non-EMV debit cards linked to accounts at Cosmos Bank to make some 12,000 international ATM withdrawals and 2,849 domestic transactions totaling \$11.5 million.

Because the attackers had previously tampered with the link between the banks' ATM switch and the core banking system, the required messages and codes for authorizing the debit card withdrawals were never forwarded to the core banking system. So typical checks on card number, card status, and PIN were never conducted. Instead, the attackers used the rogue ATM/POS switch that they had installed to send fake instructions for authorizing the fraudulent transactions.

About two days after the initial break-in, the attackers gained access to Cosmos Banks' SWIFT environment and used it to illegally transfer \$2 million to an account belonging to a trading company at Hang Seng Bank in Hong Kong.

The attack on Cosmos Bank's ATM network was different from typical jackpotting and black box attacks where attackers physically tamper with ATMs to get them to spit out large amounts of cash. In this case, the attack targeted the bank's core infrastructure and

effectively bypassed all measures recommended by the Interpol for protecting a bank's ATM infrastructure against logical attacks, Securonix said.

What remains unclear is why Cosmos Bank did not receive any alerts when the connection between its ATM switch and core banking system was cut or when thousands of ATM transactions that were clearly not normal were being made.

"We do not know for certain, but it is likely that the connection was redirected such that the connection remained active, and only the malicious requests in question were selectively redirected by the malicious component," Kolesnikov says. This would ensure that the malicious requests never made it to the legitimate payment switch, and therefore were never visible at the core backend system, he says.

The attack also likely involved a lot of malicious and suspicious attack behaviors that the bank should have spotted.

Based on the publicly available details, the attackers had to stand up a proxy switch capable of responding to malicious transaction requests from the terminals, Kolesnikov says.

They also likely had to install some targeted malware components needed to monitor the card management process and the payment infrastructure, to gain access to the SWIFT terminals and to understand the standard operating procedures.

Related Content:



Black Hat Europe

returns to London Dec 3-6 2018 with hands-on technical Trainings, cutting-edge Briefings, Arsenal open-source tool demonstrations, top-tier security solutions and service providers in the Business Hall. Click for information on the conference and to register.

Vulnerabilities/Threats Threat Intelligence Vulnerability Management Advanced Threats

Keep up with the latest cybersecurity threats, newly-discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

Subscribe