DARKReading | SIGN UP FOR OUR NEWSLETTERS

ATTACKS/BREACHES

8/27/2018
05:30 PM

Jai Vijayan
News

Connect Directly

0 COMMENTS
COMMENT NOW

Login
100% 0%

Like | Tweet | Share

North Korean Hacking Group Steals $13.5 Million From Indian Bank

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

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 Withdrawls

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:

- Thieves Target ATMs In First US 'Jackpotting' Attacks
- The Future Of ATM Hacking
- Cybercriminals Battle Against Banks' Incident Response
- 6 Reasons Security Awareness Programs Go Wrong

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.

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts
- Cyber Attack Evasion Techniques
- 5 Steps to Integrate SAST into the DevSecOps Pipeline

MORE WEBCASTS

White Papers
- Simplify Your App Security
- NetFlow vs Packet Data

MORE WHITE PAPERS

Reports
- 2020 IT Salary Survey Results Revealed
- [Report] DevSecOps & Secure App Delivery: What's Working & What's Not

MORE REPORTS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Be the first to post a comment regarding this story.

HOT TOPICS | EDITORS' CHOICE

Many Ransomware Attacks Can be Stopped Before They Begin 3
Jai Vijayan, Contributing Writer, 3/17/2020

This Tax Season, Save the Scorn and Protect Customers from Phishing Scams 2
Dr. Salvatore Stolfo, Founder & CTO, Allure Security, 3/17/2020

Fewer Vulnerabilities in Web Frameworks, but Exploits Remain Steady 1
Robert Lemos, Contributing Writer, 3/16/2020

SUBSCRIBE TO NEWSLETTERS

WEBINARS

Chatbots for the Enterprise

The ROI Story: Identifying & Justifying Disruptive Technology

The 6 Must-Haves for Practical Cloud Security

WEBINAR ARCHIVES

WHITE PAPERS

- 2020 IT Salary Survey Results Revealed
- Simplify Your App Security
- NetFlow vs Packet Data
- Anatomy of a Cloud-Native Data Breach
- Network Traffic Analysis Instrumentation Guide

MORE WHITE PAPERS

VIDEO

Ransomware Trains Its Sights on Cloud ...
6 COMMENTS

Qualys Launches Free App for IT Asset ...
1 COMMENTS

ALL VIDEOS

CARTOON

HR
klossner
" WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."

Latest Comment: Unfortunately nobody wants to spend money on security. Usually they change their mind but often it is too late

CARTOON ARCHIVE

CURRENT ISSUE

6 Emerging Cyber Threats That Enterprises Face in 2020

This Tech Digest gives an in-depth look at six emerging cyber threats that enterprises could face in 2020. Download your copy today!

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

Has the U.S. political climate caused you to make infosecurity-related changes to your disaster recovery/business continuity plans?

○ Yes

○ No

○ No but we are considering it

○ Still waiting for cybersecurity guidance from Trump admin EO

○ Don't know

○ Other (Please explain in the comments)

Submit

ALL POLLS

REPORTS

State of Cybersecurity Incident Response

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents. Read this report to find out more.

DOWNLOAD NOW!

How Enterprises Are Developing and Maintaining Secure Applications 0 COMMENTS

How Enterprises are Attacking the Cybersecurity Problem 0 COMMENTS

How Data Breaches affect the Enterprise 0 COMMENTS

MORE REPORTS

TWITTER FEED

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2019-5104**
  PUBLISHED: 2020-03-19
  ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-9013. Reason: This candidate is a duplicate of CVE-2019-9013. Notes: All CVE users should reference CVE-2019-9013 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental u...
- **CVE-2020-10678**
  PUBLISHED: 2020-03-19
  In Octopus Deploy before 2020.1.5, for customers running on-premises Active Directory linked to their Octopus server, an authenticated user can leverage a bug to escalate privileges.
- **CVE-2019-12416**
  PUBLISHED: 2020-03-19
  we got reports for 2 injection attacks against the DeltaSpike windowhandler.js. This is only active if a developer selected the ClientSideWindowStrategy which is not the default.
- **CVE-2019-20524**
  PUBLISHED: 2020-03-19
  ilchCMS 2.1.23 allows XSS via the index.php/partner/index Banner parameter.
- **CVE-2019-20527**
  PUBLISHED: 2020-03-19
  Ignite Realtime Openfire 4.4.1 allows XSS via the setup/setup-datasource-standard.jsp serverURL parameter.